

# INFORMATION PRESENTATION SYSTEM AND DEVICE

Publication number: JP2002041347

Publication date: 2002-02-08

Inventor: KIRIHATA YASUHIRO

Applicant: HITACHI SOFTWARE ENG

Classification:

- International: G06F12/14; G06F12/00; G06F15/00; G06F21/20;  
G06F21/24; G09C1/00; G06F12/14; G06F12/00;  
G06F15/00; G06F21/00; G06F21/20; G09C1/00; (IPC1-  
7): G06F12/00; G06F12/14; G06F15/00

- European:

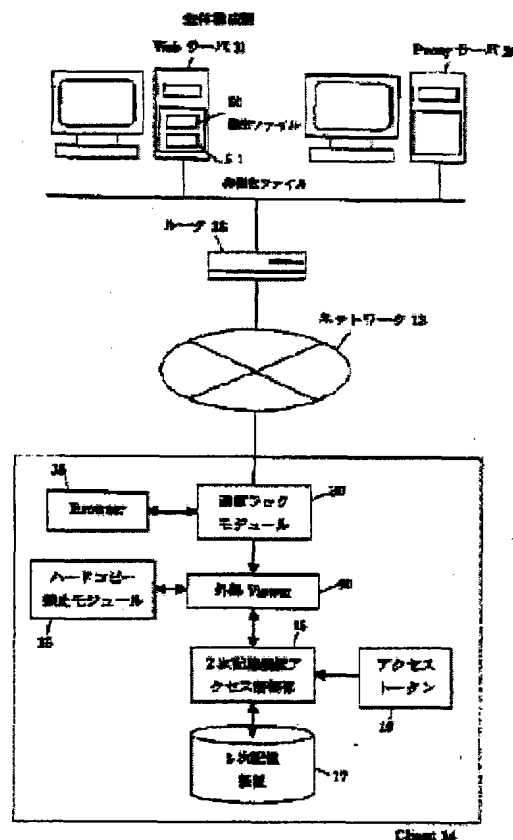
Application number: JP20010062780 20010307

Priority number(s): JP20010062780 20010307; JP20000144304 20000517

Report a data error here

## Abstract of JP2002041347

**PROBLEM TO BE SOLVED:** To enable only a person having an access right via a network to browse confidential information in a data base constructed on the existing Web server similar to a general page without altering the existing Web server and without depending on hardware structure of a device such as a client computer at a requesting origin. **SOLUTION:** This system is provided with a repeater to accept a transfer request from the device at the requesting origin to presentation object data held by a computer via the network, to authenticate the access right of the device at the requesting origin itself or a user at the requesting origin, to acquire the presentation object data from the computer according to the result of the authentication and to transfer the data to the device at the requesting origin.



Data supplied from the esp@cenet database - Worldwide

(11) 特許出願公開番号

特開2002-41347

(P2002-41347A)

(43)公開日 平成14年2月8日(2002.2.8)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	デマンド* (参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 A 5 B 0 1 7
	5 4 6		5 4 6 T 5 B 0 8 2
12/14	3 2 0	12/14	3 2 0 B 5 B 0 8 5
			3 2 0 A
15/00	3 3 0	15/00	3 3 0 D

審査請求 未請求 請求項の数27 O L (全 40 頁)

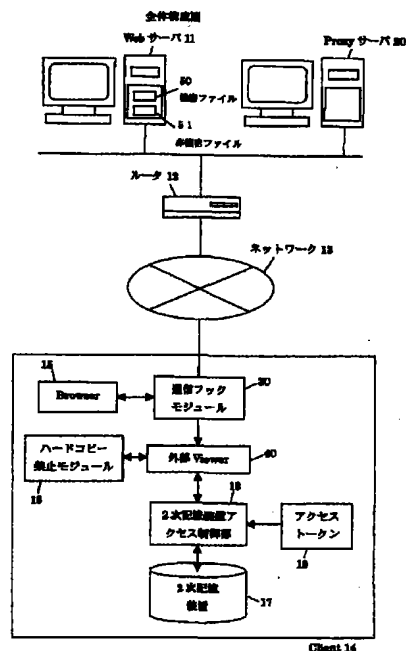
(21)出願番号	特願2001-62780(P2001-62780)	(71)出願人	000233055 日立ソフトウエアエンジニアリング株式会社 神奈川県横浜市中区尾上町6丁目81番地
(22)出願日	平成13年3月7日(2001.3.7)	(72)発明者	桐畑 康裕 神奈川県横浜市中区尾上町6丁目81番地 日立ソフトウエアエンジニアリング株式会社内
(31)優先権主張番号	特願2000-144304(P2000-144304)	(74)代理人	100088720 弁理士 小川 眞一
(32)優先日	平成12年5月17日(2000.5.17)		
(33)優先権主張国	日本(JP)		
		Fターム(参考)	5B017 AA07 BA06 CA16 5B082 EA11 GB02 5B085 AE06 BG07

(54) 【発明の名称】 情報提供システムおよび装置

(57)【要約】

【課題】 既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすること。

【解決手段】 ネットワークを介してコンピュータが保持している提供対象データに対する要求元装置からの転送要求を受け付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備える。



Client 14

## 【特許請求の範囲】

【請求項 1】 コンピュータが保持している提供対象のデータをネットワークを介して要求元装置に転送する情報提供システムであって、

ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受け付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備えることを特徴とする情報提供システム。

【請求項 2】 前記コンピュータはアクセス権限の認証を必要とする第 1 の提供対象データと、認証を必要としない第 2 の提供対象データとを保持するものであり、前記中継装置は前記第 1 の提供対象データに対する転送要求を受け付け時にアクセス権限の認証を行なうことを特徴とする請求項 1 記載の情報提供システム。

【請求項 3】 前記中継装置は、要求元装置に転送する第 1 の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする請求項 2 記載の情報提供システム。

【請求項 4】 前記要求元装置は、前記中継装置から受信した暗号化された第 1 の提供対象データを自装置または要求元ユーザに固有の暗号鍵に対応した復号鍵で復号する復号処理手段と、復号された第 1 の提供対象データを出力する第 1 の出力手段と、中継装置から受信した前記第 2 の提供対象データを出力する第 2 の出力手段を備えることを特徴とする請求項 3 記載の情報提供システム。

【請求項 5】 前記要求元装置は、前記中継装置から受信したデータに付加されている識別子により第 1 の提供対象データであるか、第 2 の提供対象データであるかを判定し、第 1 の提供対象データである場合に前記第 1 の出力手段を起動する手段と、第 1 の出力手段が正常に起動できなければ中継装置から受信した第 1 の提供対象データを削除する手段とを備えることを特徴とする請求項 4 記載の情報提供システム。

【請求項 6】 前記要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第 1 の提供対象データを暗号化して 2 次記憶装置に保管する手段とを備えることを特徴とする請求項 4 または 5 記載の情報提供システム。

【請求項 7】 前記要求元装置は、前記第 1 の出力手段に出力された第 1 の提供対象データのハードコピーを禁止する手段を備えることを特徴とする請求項 4 ～ 6 のいずれか一項に記載の情報提供システム。

【請求項 8】 前記要求元装置は、要求元装置内のアプリケーションから前記 2 次記憶装置への入出力を監視

し、前記第 1 の出力手段を介在しない第 1 の提供対象データに対するアクセスを禁止する 2 次記憶アクセス制御手段とを備えることを特徴とする請求項 7 記載の情報提供システム。

【請求項 9】 前記要求元装置は、前記ハードコピーを禁止する手段及び前記 2 次記憶アクセス制御手段が共に正常に動作していない限り前記第 1 の出力手段を起動させない手段を備えることを特徴とする請求項 8 記載の情報提供システム。

10 【請求項 10】 前記中継装置および要求元装置は、要求元装置のユーザのアクセス権限の認証を行なうためのアクセス権限判定用情報を記憶した第 1 の記憶手段をそれぞれ備えることを特徴とする請求項 6 記載の情報提供システム。

【請求項 11】 前記要求元装置は、前記 2 次記憶装置に保管された第 1 の提供対象データへのアクセスの都度または所定の時期に、前記中継装置内の前記第 1 の記憶手段に記憶されたアクセス権限判定用情報を取得し、自装置内の第 1 の記憶手段に記憶されているアクセス権限判定用情報を最新バージョンに更新する手段とを備え、更新されたアクセス権限判定用情報により、前記 2 次記憶装置に保管された第 1 の提供対象データへのアクセス権限の有無を判定することを特徴とする請求項 10 記載の情報提供システム。

【請求項 12】 前記中継装置は、要求元装置からの転送要求に付加されている要求元装置識別情報によってアクセス権限の認証を行なうことを特徴とする請求項 1 ～ 9 のいずれか一項に記載の情報提供システム。

30 【請求項 13】 前記中継装置は、要求元装置からユーザ識別情報を取得してアクセス権限の認証を行なうことを特徴とする請求項 1 ～ 9 のいずれか一項に記載の情報提供システム。

【請求項 14】 前記中継装置は、要求元ユーザのデジタルコンテンツへのアクセスに際して、アクセスに対する課金のためのアクセス記録を採取する手段を備えることを特徴とする請求項 1 ～ 13 のいずれか一項に記載の情報提供システム。

40 【請求項 15】 前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする請求項 2 記載の情報提供システム。

【請求項 16】 前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする請求項 15 記載の情報提供システム。

50 【請求項 17】 前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵

を用いて暗号化して２次記憶装置に保管する手段を備えることを特徴とする請求項１６記載の情報提供システム。

【請求項１８】 コンピュータが保持している提供対象のデータをネットワークを介して要求元装置に転送する装置であって、ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受け付け、当該要求元装置またはユーザのアクセス権限の認証を行なう手段と、アクセス権限の認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する手段を備えることを特徴とする情報提供中継装置。

【請求項１９】 要求元装置に転送する第１の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする請求項１８記載の情報提供中継装置。

【請求項２０】 要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする請求項１８記載の情報提供中継装置。

【請求項２１】 ネットワーク上のコンピュータが保持しているデータに対するアクセス権限の認証を行なう中継装置を介してアクセスし、出力する情報処理装置であって、アクセス権限の認証を必要とする第１の提供対象データを出力する第１の出力手段と、アクセス権限の認証を必要としない第２の提供対象データを出力する第２の出力手段と、アクセス対象のデータの転送要求を前記中継装置に送信する手段と、前記中継装置におけるアクセス権限の認証結果に応じて当該中継装置を介してアクセス対象のデータを受信する手段と、受信したデータが前記第１の提供対象データであれば前記第１の出力手段を起動して出力させる手段とを備えることを特徴とする情報処理装置。

【請求項２２】 前記第１の提供対象データが要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化されたものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする請求項２１記載の情報処理装置。

【請求項２３】 前記第１の提供対象データがデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で暗号化したものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする請求項２１記載の情報処理装置。

【請求項２４】 前記暗号化された第１の提供対象データを保管する２次記憶装置と、前記第１の出力手段に出力された第１の提供対象データのハードコピーを禁止す

る手段と、自装置内のアプリケーションから前記２次記憶装置への入出力を監視し、前記第１の出力手段を介しない第１の提供対象データに対するアクセスを禁止する２次記憶アクセス制御手段とを備えることを特徴とする請求項２３記載の情報処理装置。

【請求項２５】 前記ハードコピーを禁止する手段及び前記２次記憶アクセス制御手段が共に正常に動作していない限り前記第１の出力手段を起動させない手段を備えることを特徴とする請求項２４記載の情報処理装置。

【請求項２６】 自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して前記２次記憶装置に保管する手段とを備えることを特徴とする請求項２４記載の情報処理装置。

【請求項２７】 要求元ユーザの機密情報を元に生成された固有の鍵を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段を備えることを特徴とする請求項２４記載の情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する分野】本発明は、ネットワーク上に配置されたコンピュータ、例えばWebサーバ上に保管された情報をクライアントコンピュータなどの端末装置からの要求に応じて転送（または配布）し、ユーザの閲覧に供する情報提供システムに係り、特に、機密情報を正当なアクセス権限を有する者以外に漏洩することなく閲覧可能にする情報提供システムおよび装置に関するものである。

【０００２】

【従来の技術】インターネットの需要が高まるにしたがい、インターネット上で送受信される情報を保護する必要性が要求されている。例えば、一般企業等において、顧客情報や人事管理情報などの機密情報を蓄積したデータベースをWebサーバ上に構築し、社内の特別の権限を付与された者のみが自由に閲覧できるようにするシステムをインターネットの利用により容易に実現することができる。しかしながら、インターネットでは回線を盗聴したり、機密情報の蓄積されたデータベースに不正にアクセスすることにより、機密情報が盗まれる恐れがある。また、機密情報にアクセスすることを許された特権のある人物が機密情報にアクセスしてその機密情報をコピーし、第３者に漏洩してしまう事件も発生している。このようなことから、インターネット上のWebサーバ等に蓄積された機密情報を正当なアクセス権限を有する者以外に漏洩することなく閲覧可能にするシステムの実現が強く望まれている。

【０００３】従来、機密情報を管理し漏洩を防止するシステムとして、例えば特開平１１－３２８１２０号公報に記載のものが知られている。特開平１１－３２８１２

10

20

30

40

50

0号公報に記載のものは、端末装置の入出力機器の構成や利用者等のデータによって、機密情報の格納されたデータベースへのアクセス権を予め設定し、データベース内の機密情報の漏洩を防ぐためのネットワークシステムである。

【0004】具体的に図40を用いて説明すると、ホストコンピュータA02は端末装置A05からの通信要求を受けると、照合部A09にて利用者識別子記憶部A08に登録されている利用者識別子との照合を行なう。照合結果が一致すると、端末装置A05へハードウェア構成情報を要求する。端末装置A05からハードウェア構成情報を受信すると、照合部A09にて端末構成情報記憶部A10に記憶されているハードウェア構成情報と照合を行い、照合結果が一致すると、端末装置A05のデータベースA11、A12へのアクセス権の有無を判定部A13に行なわせる。判定部A13から判定結果を受けた制御部A15は以後、端末装置A05にアクセス権の有るデータベースの使用を許可するというシステムである。

【0005】一方、デジタルコンテンツに課金して、利用者に配信するサービスはすでにWeb上で試みられている。例えば、利用者がWebブラウザを使用してバーチャルモール等のデジタルコンテンツ配信ページにアクセスし、バーチャルモールに置かれたデジタルコンテンツを、Webブラウザを使用してダウンロードする方法がある。この方式では、利用者は予めデジタルコンテンツ配信を行っているサイトの管理会社にデジタルコンテンツ配信サービスを受けるための登録を行なう。登録はクレジットカード等の情報を使用してWeb上で行なう方法や、申請書を郵送で送付する方法などがある。登録が済むと、サイトの管理会社からデジタルコンテンツにアクセスするためのIDとパスワードが発行される。デジタルコンテンツはWebサーバに保管されており、デジタルコンテンツにアクセスするためにはProxyサーバ経由でアクセスしなければならない。アクセス時に、利用者はIDとパスワードによりProxyサーバで認証され、認証が成功すれば利用者はデジタルコンテンツにアクセスできる。

【0006】しかしながら、この方式における重大な問題点として、利用者によるデジタルコンテンツの不正な二次利用・再配布が考えられる。すなわち、Webブラウザでダウンロードしたデジタルコンテンツをファイルとして保存し、そのファイルをホームページに掲載する、もしくはFTPやメール等を利用して配布する等の行為である。このような行為により、コンテンツ料金を支払っていないにも拘わらず、そのデジタルコンテンツを使用できるユーザが現れ、デジタルコンテンツの課金サービスが成立しない。

【0007】この問題点に対する解決策として、デジタルコンテンツに電子透かしを入れる方法が考えられる。

例えば画像コンテンツの場合、画像データに独自のロゴを埋め込む可視の電子透かしや、輝度の変化を利用して画像データに目立たない形で情報を埋め込む不可視の電子透かしなどがある。また、コンテンツの利用条件に違反した二次利用や不正な再配布を防止する従来技術として、特願平10-190343号には、電子透かしの著作物への埋め込みとその検出についての技術が開示されている。

【0008】

【発明が解決しようとする課題】しかしながら、上記の特開平11-328120号公報に記載のものは、一般のWebサーバ11上に構築されたデータベースに対して適用する場合、既存のWebサーバを改変せねばならず、現在運用されている一般的なWebサーバ上のデータベースに適用するには手間がかかるという問題がある。また、Webサーバには、通常、機密情報以外に一般に閲覧するページも存在しており、こうした一般のページの閲覧に対応できない。さらに、ハードウェア構成により機密ファイルのダウンロードを許可する仕組みであるため、適切なハードウェア条件を満たしていなければ、機密ファイルを閲覧することができず、閲覧した機密情報データを一時的に端末に保持しておく機構もない。

【0009】一方、上述の電子透かしによるデジタルコンテンツの二次利用・再配布を防止する方式にはいくつかの課題がある。まず、透かしを除去して配信する可能性がある。可視の電子透かしの場合にはこの脅威に対する解決策はなく、あくまで抑止効果を期待しているに過ぎないといえる。不可視な電子透かしについては、透かしの除去は困難であるが、一般的に画像データの回転処理や部分的な切り取り等の加工処理に対して弱いとされており、そのような加工処理により電子透かしが検出できなくなったという例も報告されている。また、不正な二次利用・再配布を摘発するために、インターネット上にある画像データに透かしがあるかどうかを検出する必要があるが、検出するための有効な方法が確立されていない。さらに、記録媒体に記録して、オフラインでデジタルコンテンツを配布する場合に対しては、透かしの効果はまったく期待できない。従って、電子透かしを利用した二次配信の防止は抑止効果を期待した消極的な方法であると言える。

【0010】本発明の第1の目的は、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置（または端末）のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすることができる情報提供システムおよび装置を提供することにある。

【0011】本発明の第2の目的は、閲覧した機密情報を第3者に漏洩しないように要求元装置内に保存・管理

することができる情報提供システムおよび装置を提供することにある。本発明の第3の目的は、デジタルコンテンツをダウンロードした利用者がダウンロードに使用したマシンでしかデジタルコンテンツを利用できず、ダウンロードしたデジタルコンテンツの不正な二次利用・再配布を防止することができる情報提供システムおよび装置を提供することにある。

【0012】

【課題を解決するための手段】上記の第1の目的を達成するために、本発明は、ネットワークを介してコンピュータ（例えばWebサーバ）が保持している提供対象データに対する要求元装置（例えばクライアントコンピュータ）からの転送要求を受け付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備えることを特徴とする。また、前記コンピュータはアクセス権限の認証を必要とする第1の提供対象データと認証を必要としない第2の提供対象データとを保持するものであり、前記中継装置は前記第1の提供対象データに対する転送要求を受け付け時にアクセス権限の認証を行なうことを特徴とする。また、前記中継装置は、要求元装置に転送する第1の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化された第1の提供対象データを自装置または要求元ユーザに固有の暗号鍵に対応した復号鍵で復号する復号処理手段と、復号された第1の提供対象データを表示する第1の表示手段と、中継装置から受信した前記第2の提供対象データを表示する第2の表示手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信したデータに付加されている識別子により第1の提供対象データであるか、第2の提供対象データであるかを判定し、第1の提供対象データである場合に前記第1の表示手段を起動する手段と、第1の表示手段が正常に起動できなければ中継装置から受信した第1の提供対象データを削除する手段とを備えることを特徴とする。

【0013】上記第2の目的を達成するために、前記要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第1の提供対象データを暗号化して2次記憶装置に保管する手段とを備えることを特徴とする。また、前記要求元装置は、前記第1の出力手段に出力された第1の提供対象データのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、要求元装置内のアプリケーションから前記2次記憶装置への入出力を監視し、前記第1の出力手段を介しない第1の提供対象データに対するアクセスを禁止す

る2次記憶アクセス制御手段とを備えることを特徴とする。また、前記要求元装置は、前記ハードコピーを禁止する手段及び前記2次記憶アクセス制御手段が共に正常に動作していない限り前記第1の出力手段を起動させない手段を備えることを特徴とする。また、前記中継装置および要求元装置は、要求元装置のユーザのアクセス権限の認証を行なうためのアクセス権限判定用情報を記憶した第1の記憶手段をそれぞれ備えることを特徴とする。また、前記要求元装置は、前記2次記憶装置に保管された第1の提供対象データへのアクセスの都度または所定の時期に、前記中継装置内の前記第1の記憶手段に記憶されたアクセス権限判定用情報を取得し、自装置内の第1の記憶手段に記憶されているアクセス権限判定用情報を最新バージョンに更新する手段とを備え、更新されたアクセス権限判定用情報により、前記2次記憶装置に保管された第1の提供対象データへのアクセス権限の有無を判定することを特徴とする。また、前記中継装置は、要求元装置からユーザ識別情報を取得してアクセス権限の認証を行なうことを特徴とする。また、前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化して2次記憶装置に保管する手段を備えることを特徴とする。

【0014】上記第3の目的を達成するために、本発明における要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第1の提供対象データを暗号化して2次記憶装置に保管する手段とを備えることを特徴とする。また、前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化して2次記憶装置に保管する手段を備えることを特徴とする。

【0015】本発明の情報提供中継装置は、ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受け、当該要求元装置またはユーザのアクセス権限の認証を行なう手段と、アクセス権限の認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する手段を備えることを特徴とする。また、要求元装置に転送する第1の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする。また、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。

【0016】また、要求元装置を構成する情報処理装置は、アクセス権限の認証を必要とする第1の提供対象データを出力する第1の出力手段と、アクセス権限の認証を必要としない第2の提供対象データを出力する第2の出力手段と、アクセス対象のデータの転送要求を前記中継装置に送信する手段と、前記中継装置におけるアクセス権限の認証結果に応じて当該中継装置を介してアクセス対象のデータを受信する手段と、受信したデータが前記第1の提供対象データであれば前記第1の出力手段を起動して出力させる手段とを備えることを特徴とする。また、前記第1の提供対象データが要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化されたものであり、該暗号化された第1の提供対象データを復号した後に前記第1の出力手段に出力させる復号処理手段を備えることを特徴とする。また、前記第1の提供対象データがデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で暗号化したものであり、該暗号化された第1の提供対象データを復号した後に前記第1の出力手段に出力させる復号処理手段を備えることを特徴とする。また、前記暗号化された第1の提供対象データを保管する2次記憶装置と、前記第1の出力手段に出力された第1の提供対象データのハードコピーを禁止する手段と、自装置内のアプリケーションから前記2次記憶装置への入出力を監視し、前記第1の出力手段を介しない第1の提供対象データに対するアクセスを禁止する2次記憶アクセス制御手段とを備えることを特徴とする。また、前記ハードコピーを禁止する手段及び前記2次記憶アクセス制御手段が共に正常に動作していない限り前記第1の出力手段を起動させない手段を備えることを特徴とする。また、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第1の提供対象データを暗号化して前記2次記憶装置に保管する手段とを備えることを特徴とする。また、要求元ユーザの機密情報を元に生成された固有の鍵を用いて前記第1の提供対象データを暗号化して2次記憶装置に保管する手段を備えることを

特徴とする。

【0017】

【発明の実施の形態】以下、本発明を実施する場合の一形態を図面を参照して具体的に説明する。図1は、本発明の情報提供システムの第1の実施形態を示す全体構成図であり、大別すると、Webサーバ11、ルータ12、ネットワーク13、クライアントコンピュータ（以下、Clientと略記）14およびProxyサーバ20で構成されている。Client14は、Browser15、ハードコピー禁止モジュール16、2次記憶装置17、2次記憶装置アクセス制御部18、アクセストークン19、通信フックモジュール30、外部Viewer40を備えている。

【0018】Webサーバ11は、アクセス権限の認証を必要とする機密ファイル（第1の提供対象データ）50とアクセス権限の認証を必要としない非機密ファイル（第2の提供対象データ）51を保管している。このWebサーバ11とProxyサーバ20は、同じセグメント上に配され、ルータ12によってネットワーク13から隔離されている。従って、機密ファイル50へのアクセスを行なうためには、必ずProxyサーバ20を経由しなければならない。Client14が機密ファイル50にアクセスしたとき、機密ファイル50は一旦Proxyサーバ20にダウンロードされ、Client14ごとに用意された共通鍵を用いて動的に暗号化される。

【0019】Webサーバ11上には機密ファイル50を予め暗号化して保管しておく必要はない。暗号化された機密ファイル50はClient14に送信され、通信フックモジュールにおいて復号された後、専用の外部Viewer（第1の表示手段）40に表示される。Client14内では、ユーザごとに設けられたフォルダに、対応するユーザでシステムにログインし、専用の外部Viewer40でしかアクセスできないようなアクセス制御をOSレベルで行なうようになっている。従って、ユーザごとに機密ファイルの管理が行なえる機構を備えたシステムであると言える。

【0020】次に、各構成要素について説明する。Webサーバ11はHTTPプロトコルもしくはFTPプロトコル等によってClient14よりProxyサーバ20経由で送られるファイルのダウンロード要求を処理し、Client14にファイルを転送する機能を有するものであり、同時にユーザ認証も行なう。ルータ12は、IPパケットの宛先IPアドレスによるフィルタリングを行っており、Proxyサーバ20へ送信されるIPパケットのみ通過させるように設定されている。従って、Webサーバ11へのアクセスは、すべてProxyサーバ20を介して行われる。Proxyサーバ20はClient14からのアクセスを解析し、機密ファイル50へのアクセスの場合にはダウンロードした機密ファイル50をClient14ごとに用意された共通鍵を用いて暗号化し、Client14に転送する。Browser15は、Webサーバ11からダウンロードし

たファイル、又はプログラムを表示、ないしは実行するためのアプリケーションであり、機密ファイル50以外の一般のファイル51を閲覧する際に使用する。

【0021】通信フックモジュール30は、Proxyサーバ20にClient14を認証させるためのClientマシン識別子を付加してファイルのGETリクエストを送信し、ダウンロードされた暗号化された機密ファイル50を復号する。外部Viewer40は、機密ファイル50がダウンロードされてきた際に通信フックモジュール30によって起動され、復号された機密ファイル50を表示し、2次記憶装置17に保存したり、読み出す処理を行なう。ここで、外部Viewer40は表示データのコピー機能（マウスカーソルによる選択、もしくはDrag&Dropによるコピー）を実装しない。ハードコピー禁止モジュール16は、外部Viewer40が起動されると同時に起動され、終了すると同時に終了するモジュールであり、システムコールをフックする機能を利用することにより（例えばWindows NTではWin32 Hooksを利用）、ハードコピーを禁止する機能を有する。

【0022】2次記憶装置アクセス制御部18は、OSの起動時にロードされるモジュールであり、アプリケーションが2次記憶装置17にアクセスする際に出される入出力要求を途中で捕獲し解析し、アクセス要求ファイル、アクセス要求アプリケーションを確定し、特定のフォルダ内のファイルに対するアクセスの場合には外部Viewer40のみにしかアクセスできないように制限を加える。フォルダは機密ファイル閲覧者ごとに用意されており、2次記憶装置アクセス制御部18はアクセストークン19を調べることにより、ユーザアカウントごとに各フォルダに対してアクセス制限をかける機能を有する。アクセストークン19は、ユーザがClient14にログインした時点でOS内部に生成されるオブジェクトであり、OSにおけるユーザのログイン情報を管理し、OSの機能として持つファイルへのユーザごとのアクセス制限のためにも使用される。

【0023】図2は、本発明におけるProxyサーバ20のブロック構成図である。Proxyサーバ20は、Client14とProxyサーバ20間の通信を司るClient-Proxy間通信制御部21と、Webサーバ11上に保管されている機密ファイル50のURLが登録されている機密ファイルURL登録部22と、通信フックモジュール30を有するClient14を認証するためのClientマシン識別子が格納されたClientマシン識別子データベース23と、Client14から送信されたデータを解析して、機密ファイル50へのアクセスかどうかを判定するProxy内受信データ解析部24と、Client14から送られたデータ内にClientマシン識別子があるかどうかを判定するClientマシン認証部25と、Webサーバ11とProxyサーバ20間の通信を司るWeb-Proxy間通信制御部26と、Proxyサーバ20からClient14への送信ファイルが機密ファイ

ル50を暗号化したものであることをClient14に知らせるために識別子を付加する機密ファイル識別子付加部27と、Webサーバ11からダウンロードした機密ファイル50を暗号化する機密ファイル暗号化部28と、暗号化のためにClient14ごとに用意された共通鍵を管理する共通鍵データベース29で構成されている。

【0024】図3は、Client14内に設けた通信フックモジュール30のブロック構成図である。図3において、Proxy-通信フックモジュール間通信制御部31は、Proxyサーバ20と通信フックモジュール30との間の通信を司る部分である。機密ファイル識別子格納部32は、Proxyサーバ20において、機密ファイル50に付加された機密ファイル識別子を照合するために、予め識別子のコピーを格納しておく部分である。また、受信データ解析部35は、通信フックモジュール30が受信したデータを解析し、データ内に暗号化された機密ファイル50であることを示す機密ファイル識別子が存在するか否かを確認するものであり、機密ファイル識別子が存在すれば、受信データ解析部35は受信データを暗号化ファイル復号部33に渡し、機密ファイル識別子が存在しなければ、受信データを内部アプリケーション-通信フックモジュール間通信制御部37に渡す。

【0025】暗号化ファイル復号部33は、共通鍵格納部34に格納されているClient14固有の共通鍵を用いて、暗号化された機密ファイル50を復号する。送信データ解析部36は、GETリクエストの送信先URLを調べて、Proxyサーバ20への送信の場合はClientマシン識別子付加部38に送信データを渡す。Clientマシン識別子付加部38は、送信データに各Client14固有のClientマシン識別子を付加する。外部Viewer起動処理部39は、暗号化ファイル復号部33より要請を受けて、外部Viewer40を起動し、起動できたかどうかを暗号化ファイル復号部33に知らせる。

【0026】図4はClient14内に設けた外部Viewer40のブロック構成図である。図4において、通信フックモジュール-Viewer間通信制御部41は、通信フックモジュール30と外部Viewer40との間の通信を司るものである。機密ファイル表示部42は、機密ファイルキャッシュ部43にキャッシュされた機密ファイル50を表示するものである。機密ファイルキャッシュ部43は外部Viewer40に転送された機密ファイル50を一時的に保存しておく所である。機密ファイルアクセス・保存処理部44は、機密ファイルキャッシュ部43にキャッシュされている機密ファイル50を2次記憶装置17内に保存したり、2次記憶装置17内に保存されている機密ファイル50にアクセスしたりする。

【0027】外部Viewer起動判定部47は、ハードコピー禁止モジュール起動処理部45、及び2次記憶装置アクセス制御部起動処理部46にアクセスして、ハードコピー禁止モジュール16を起動、また2次記憶装置ア



セス制御部18が起動しているか否かの確認を行い、通信フックモジュール30に通知する。

【0028】次に、本実施形態における各モジュール間の処理の流れや関連を説明する。図5はProxyサーバ20における処理のフローチャートを示したものである。Proxyサーバ20は、Client14からのアクセスがあると(ステップ501)、Proxy内受信データ解析部24で受信したデータの解析を行い、アクセス要求ファイルのURLやClientマシン識別子の有無等を調べる(ステップ502)。そしてアクセス要求ファイルのURLと機密ファイルURL登録部22にある機密ファイルURLのデータをもとに、機密ファイル50へのアクセス要求であるかどうか調べる(ステップ503)。機密ファイル50へのアクセスでない場合、受信データにClientマシン識別子があればそれを除去し、なければそのままの状態、Webサーバ11に転送する。

【0029】Webサーバ11では、ユーザ認証が行われ、認証が通ればWebサーバ11から非機密ファイル51がダウンロードされる(ステップ511)。その後、ダウンロードした非機密ファイル51をそのままClient14に転送する(ステップ512)。

【0030】アクセス権限の認証を必要とする機密ファイル50へのアクセスである場合、Clientマシン識別子が検出されていれば、Proxy内受信データ解析部24はそのClientマシン識別子をClientマシン認証部25に渡し、Clientマシン認証部25においてClientマシン識別子データベース23をもとにClientマシン認証を行なう(ステップ504)。Clientマシン識別子がClient14からの受信データに付加されていない場合は、本発明のシステムにおける正当なClient14からのアクセスでないと判断して、機密ファイル50へのアクセスを拒否する。また、Clientマシン認証部25においてClientマシンが認証されない場合も同様に機密ファイル50へのアクセスを拒否する(ステップ506)。

【0031】Clientマシン識別子が照合され、アクセス要求を行ったClient14がClientマシン識別子データベース23に予め登録されている正当なClientマシンであると認証された場合、Clientマシン認証部25から通知を受けたProxy内受信データ解析部24は、Clientマシン識別子を除去した受信データをWebサーバ11に転送し、Webサーバ11から該当する機密ファイル50をダウンロードする(ステップ507)。

【0032】この後、機密ファイル暗号化部28にて、ダウンロードした機密ファイル50を共通鍵データベース29にあるClient14に対応した共通鍵を用いて暗号化し(ステップ508)、さらに機密ファイル識別子付加部27にて暗号化された機密ファイルに機密ファイル識別子を付加した後(ステップ509)、その暗号化され、かつ識別子の付加された機密ファイルをClient14に転送する(ステップ510)。なお、共通鍵データベ

ース29内のClient14に対応した共通鍵を検索するとき、Clientマシン認証部25から得たClient14の認証結果をもとに行なう。共通鍵データベース29内の共通鍵とClientマシン識別子とは1対1に対応付けられている。

【0033】図6は、Client14内の通信フックモジュール30におけるデータ送信時の一連の処理を記述したフローチャートである。まず、Browser15からネットワーク13へデータが送信された場合、内部アプリケーション-通信フックモジュール間通信制御部37にてそのデータを受信し(ステップ601)、送信データ解析部36で送信データを解析し、送信先がProxyサーバ20であるかどうかを調べる(ステップ602)。Proxyサーバ20への送信でなければ、送信データをネットワーク13にそのまま転送する(ステップ604)。Proxyサーバ20への送信であれば、Clientマシン識別子付加部38において送信データにClientマシン識別子を付加した後(ステップ605)、Proxyサーバ20に送信データを転送する(ステップ606)。

【0034】図7は、通信フックモジュール30において、データ受信時における処理のフローチャートである。通信フックモジュール30は、Proxy-通信フックモジュール間通信制御部31でネットワーク13からClient14に送られてきたデータを受信したならば(ステップ701)、受信データ解析部35で受信データに機密ファイル識別子があるかないかを解析する(ステップ702、703)。受信データから機密ファイル識別子が検出されなかった場合、そのままBrowser15に受信データを転送する(ステップ709)。しかし、機密ファイル識別子が検出された場合、暗号化ファイル復号部33にて、機密ファイル識別子を除去し、共通鍵格納部34に格納されているClient14に固有の共通鍵を用いて暗号化された機密ファイル50を復号する(ステップ704)。そして外部Viewer40起動処理部39により外部Viewer40が起動していなければ起動させ、外部Viewer40が正常に起動したかどうか確認させる(ステップ705、706)。外部Viewer40の起動を試みたのに起動していなければ受信データを削除する(ステップ707)。外部Viewer40が正常に起動していれば、復号された機密ファイル50のデータを外部Viewer40に転送して表示させる(ステップ708)。

【0035】図8は、2次記憶装置アクセス制御部18における機密ファイルアクセス時の処理のフローチャートである。2次記憶装置17にはユーザごとに用意された機密ファイル保存用の特別なフォルダがあるとする。このフォルダは各ユーザのアカウントと一緒に2次記憶装置アクセス制御部18に登録されているものであり、この登録データをもとに2次記憶装置アクセス制御部18は、Client14にログインしているユーザがこのフォルダにアクセスできるかどうかを判定する。Client14

内のアプリケーションから、2次記憶装置17の特定のフォルダに保存された機密ファイル50へのアクセス要求があったとき、機密ファイル50へのI/Oアクセス要求がシステム内部で出され、2次記憶装置17に送られるが、2次記憶装置アクセス制御部18はそのI/Oアクセス要求を途中でフックし、その内容を解析する(ステップ801)。この解析により、I/Oアクセス要求を行っているアプリケーションとアクセス要求フォルダを調べる。2次記憶装置アクセス制御部18はアクセストークン19にアクセスし、ログインユーザ情報を取得する(ステップ802)。

【0036】アクセス要求アプリケーションが外部Viewer40であるかどうか、アクセス要求対象のフォルダがログインユーザに対応しているかどうかを判定し、アクセス要求対象のフォルダ内の機密ファイルへアクセスしてよいかどうかを判定する。アクセス要求対象のフォルダがログインユーザに対応しているかどうかは、予め2次記憶装置アクセス制御部18にある、機密ファイル保存用フォルダへのパスとそのフォルダにアクセス可能なユーザのユーザアカウントの対データが登録されているデータベース(図示せず)を検索することで判定する(ステップ803)。アクセス可能であるならば、機密ファイル50へのアクセスを許可してI/Oアクセス要求を2次記憶装置17のデバイスドライバに渡す(ステップ805)。アクセス不可能の判定が出たならば、機密ファイル50へのアクセスを禁止する(ステップ806)。

【0037】なお、2次記憶装置17に格納された機密ファイル50へのアクセスの判定条件は、アクセス要求しているアプリケーションが外部Viewer40であり、かつアクセス要求対象の機密ファイル格納フォルダがログインユーザに対応している場合にのみアクセスを許すものとする。すなわち、機密ファイル格納フォルダがログインユーザに対応している場合であっても、外部Viewer40が起動していない状態では、2次記憶装置17に格納された機密ファイル50へのアクセスは許可しない。また、外部Viewer40が起動している状態であったとしても、機密ファイル格納フォルダがログインユーザに対応していない場合もアクセスを許可しない。

【0038】図9は、外部Viewer40における受信データ表示処理のフローチャートである。外部Viewer40は、通信フックモジュール30から起動要求を受ける、またはユーザから起動要求を受けると(ステップ901)、2次記憶装置アクセス制御部起動処理部46で、2次記憶装置アクセス制御部18が動作しているかどうか調べる(ステップ902)。動作していないならば、外部Viewer40起動判定部47は、通信フックモジュール30にエラーを通知し(ステップ903)、外部Viewer40の起動を終了する(ステップ904)。動作していれば、外部Viewer40は、ハードコピー禁止モジュール

起動処理部45でハードコピー禁止モジュール16の起動を試みる(ステップ905)。起動しなければ、外部Viewer起動判定部47は通信フックモジュール30にエラーを通知し(ステップ909)、外部Viewer40の起動を中止する(ステップ910)。ハードコピー禁止モジュール16が起動すれば、通信フックモジュール30から復号された機密ファイル50を受信し(ステップ907)、その受信データを表示する(ステップ908)。

【0039】このように外部Viewer40起動の際に、ハードコピー禁止モジュール16が起動するかどうか判定し、さらに2次記憶装置アクセス制御部18が正常に動作していることを確認することによって、外部Viewer40が復号された機密ファイル50のデータを表示する際に、機密データのハードコピーが撮られてしまうことを不可能にすることができる。さらに、予め2次記憶装置アクセス制御部18に登録してある機密ファイル格納フォルダ内に保存されている機密ファイルが別のフォルダにコピーできないことを保障することができる。そして、その機密ファイル格納フォルダには外部Viewer40でしかアクセスできないので、他のアプリケーションによって機密ファイル格納フォルダに保存された機密ファイルにアクセスすることができない。また、外部Viewer40が起動しなければ通信フックモジュール30は復号した機密ファイルを削除してしまうので、Client14内の他のアプリケーションには機密ファイル50にアクセスする手段がなく、機密データが外部に漏洩することはない。

【0040】なお、ユーザが外部Viewer40を起動した場合には、ステップ903と909の通信フックモジュールへのエラー通知は行なわない。

【0041】以上説明したように、本実施形態の情報提供システムは、機密ファイル50と非機密ファイル51を保管したWebサーバ11に対し、Client14からの機密ファイル50へのアクセス要求があった場合、Client14から送信されたアクセス要求(転送要求)に付加されているClientマシン識別子をもとにClient14の認証を行い、アクセス権限を有するClient14であれば、要求された機密ファイル50をWebサーバ11からダウンロードし、その機密ファイルをアクセス要求元のClient14に固有の共通鍵を用いて暗号化し、さらに暗号化ファイルであることを示す機密ファイル識別子を付加し、アクセス要求元のClient14に転送するProxyサーバ20を備えることを特徴とする。

【0042】このような構成により、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置(または端末)のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能に

することができる。

【0043】また、Client14において、Webサーバ11上の一般の非機密ファイル51を閲覧するためのBrowser15と、機密ファイル50を閲覧し、2次記憶装置17に保存する手段を備えた外部Viewer40と、Client14内の任意のアプリケーションとネットワーク13との通信を中継し、暗号化された機密ファイル50を受信した際に外部Viewer40を起動し、起動できなければ機密ファイル50を削除する手段と、Client14からProxyサーバ20へのデータ送信の際にClientマシン識別子を送信データに付加する手段と、Proxyサーバ20から送信された暗号化された機密ファイルを識別してClient14に固有の復号鍵で暗号化された機密ファイルを復号し、外部Viewer40に転送する手段と、機密ファイル50以外のファイルが転送されてきたとき、それを判定してBrowser15にそのデータを転送する手段とを備えた通信フックモジュール30と、ログインユーザ情報を格納したアクセストークン19と、機密情報を格納するための2次記憶装置17と、アクセストークン19からログインユーザ情報を取得する手段と、Client14内のアプリケーションから2次記憶装置17へのI/Oを監視して、ファイルへのアクセス要求を行っているアプリケーションとそのアクセス要求ファイルを特定する手段と、特定のフォルダに対して、特定のログインユーザが外部Viewer40でアクセスする以外にはアクセスを禁止する手段とを備えた2次記憶装置アクセス制御部18と、外部Viewer40起動中に外部Viewer40に表示されている画面のハードコピーを禁止する手段を備えたハードコピー禁止モジュール16とを有することを特徴とする。さらに、外部Viewer40は、ハードコピー禁止モジュール16及び2次記憶装置アクセス制御部18が共に正常に動作していない限り起動しない手段を備えることを特徴とする。

【0044】このような構成により、閲覧した機密ファイル50を第3者に漏洩しないようにアクセス要求元のClient14内に保存・管理することができる。また、機密ファイル50はClient14ごとに決められた共通鍵を用いて暗号化されて要求元のClient14に送信されるので、Client14とProxyサーバ20間の通信回線上で盗聴される恐れがなくなる。また、ダウンロードした機密ファイル50は、ユーザごとに所定のフォルダに安全に保管され、なおかつ保管された機密ファイル50は外部Viewer40以外のアプリケーションではアクセスできないために、コピーされて外部に持ち出されることもない。さらに外部Viewer40起動中にはハードコピー禁止モジュール16が起動しているため、外部Viewer40に表示されている機密データのハードコピーをとることもできなくなり、アクセス権限を有するユーザであったとしても機密データをコピーして外部に持ち出すことは不可能になる。

【0045】なお、Proxyサーバ11に対するアクセス要求にはClientマシン識別子を付加しているが、Webサーバ11における認証の仕方によってユーザ識別子と組み合わせる、あるいはユーザ識別子のみにすることができる。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵もClient14に固有のものでなく、アクセスする個々のユーザまたはユーザグループに対応するものであってもよい。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵は、Client14の装置自身に固有の情報（MACアドレス、IPアドレス、CPU製造番号など）を元に生成した鍵情報、またはユーザ自身の機密情報（例えばクレジット番号など）から生成した鍵情報を用いてもよい。

【0046】次に、本発明の第2の実施形態について説明する。図10は、第2の実施形態を示す全体構成図である。この第2の実施形態の情報提供システムは、機密ファイル50と非機密ファイル51を保管しているWebサーバ11と、機密ファイル50へのアクセス権限を策定すると共に、ユーザ及びマシン認証及びClient14からの機密ファイル50へのアクセス要求に従いWebサーバ11から機密ファイル50をダウンロードして暗号化し、アクセス要求元のClient14へ暗号化された機密ファイル50の転送を行なうProxyサーバ20と、ルータ12と、ネットワーク13と、複数のClient14によって構成されている。各Client14は、Proxyサーバ20から送られた暗号化機密ファイルのファイル名を除去し、キャッシュ、復号化して表示するViewer60、非機密ファイル51を表示するBrowser61、暗号化された機密ファイル50を復号するためのユーザ固有の復号鍵を格納した復号用共通鍵データベース62、ユーザ固有の復号用共通鍵と復号用共通鍵を適用するためのポリシーを管理する機能をもつポリシー管理モジュール64及びポリシーデータベース63を備えている。

【0047】この実施形態においても、前述した第1の実施形態と同様に、Webサーバ11とProxyサーバ20は同じセグメント上に配置されており、外部のネットワーク13とはルータ12のみを介して接続されている。ルータ12においては、IPパケットの宛先IPアドレスによるフィルタリングを行っており、Proxyサーバ20へ送信されるIPパケットのみ通過させる。また、各Client14には、ファイルの拡張子から判断してViewer60を起動するBrowser61がインストールされている。

【0048】図11は、本実施形態におけるClient14のブロック構成図である。Client14は、Viewer60、Browser61、復号用共通鍵データベース62、2次記憶装置67、ハードウェア固有情報65、ネットワーク側通信制御部66、ポリシーデータベース63、ポリシー管理モジュール64を有している。このうち、Viewer60はViewer起動判定部6011、Viewer内認証用ハードウェア固有情報6012、暗号化機密ファイルキャッシュ

部6013、機密ファイル名データ除去部6014、暗号化機密ファイル復号部6015、機密ファイル表示部6016、及びViewer内復号用共通鍵キャッシュ部6017を備えている。

【0049】Viewer起動判定部6011は予め登録しておいたViewer内認証用ハードウェア固有情報6012と、Client14のハードウェアに固有のデータであるハードウェア固有情報65（これは例えばMACアドレスや別途外付けされたハードウェア、ICカード内に貯えられた改竄不可能な特殊データなど）を比較照合し、2つのデータが一致すればViewer60を起動し、一致しなければViewer60を起動させない判定を下すモジュールである。暗号化機密ファイルキャッシュ部6013は、暗号化機密ファイル50がBrowser61から転送された際に、暗号化機密ファイル50を一時的にキャッシュしておくものである。Viewer60でファイルを2次記憶装置67に保存する場合、この暗号化機密ファイルキャッシュ部6013にキャッシュされているデータを保存する。このことにより、2次記憶装置67には機密ファイル50が暗号化されたまま保存される。保存された機密ファイル50を参照するときには、この機密ファイル50を暗号化するために用いられた、ユーザに固有の復号用共通鍵と復号するためのViewer60、復号可能な設定にあるポリシーデータが必要である。従って、2次記憶装置67に保存された暗号化機密ファイル50が、Client14から外部に漏れたとしても、復号用共通鍵データベース62に保管されるべきユーザ固有の復号用共通鍵、Viewer60、及びポリシー管理モジュール64がなければ暗号化機密ファイル50を閲覧することができず、機密情報が外部に漏れることはない。

【0050】機密ファイル名データ除去部6014は、Proxyサーバ20で機密ファイル50であることを表すためにファイル名の付け替えられた暗号化機密ファイル50がBrowser61から転送された際、この暗号化機密ファイル50のファイル名データを除去するモジュールである。暗号化機密ファイル復号部6015は、Viewer内復号用共通鍵キャッシュ部6017にキャッシュされたユーザ固有の復号用共通鍵を用いて、ファイル名データの除去された暗号化機密ファイル50を復号するものである。Viewer内復号用共通鍵キャッシュ部6017は、ポリシー管理モジュール64から渡されたユーザ固有の復号用共通鍵を一時的にキャッシュするものである。Browser61は、Proxyサーバ20から送られてきた機密ファイル50をそのファイル名から判断し、Viewer60を起動して暗号化された機密ファイル50をViewer60に転送する。ハードウェア固有情報65は、MACアドレスや別途外付けされたハードウェア、ICカード内の機密データなど、Client14マシンのハードウェア構成に固有の情報である。ネットワーク側通信制御部66は、Client14をネットワーク13に接続するための通

信制御モジュールである。ポリシーデータベース63は、Proxyサーバ20で管理されている機密ファイル50へのアクセスポリシー（アクセス権限を判定するための情報）をダウンロードし、暗号化して保管しておくところであり、2次記憶装置67に保存されている暗号化された機密ファイル50を閲覧するために、Viewer60及びポリシー管理モジュール64を起動する際にProxyサーバ20と通信して更新される。

【0051】図12は、本実施形態におけるProxyサーバ20のブロック構成図である。Proxyサーバ20は、Client-Proxy間通信制御部201、機密ファイルリスト及びアクセスポリシー登録部202、要求ファイルアクセス判定部203、受信データ解析部204、ユーザ認証部205、暗号用共通鍵選択部206、機密ファイル暗号部207、Web-Proxy間通信制御部208、機密ファイルキャッシュ部209、機密ファイルURL送信部210、暗号用共通鍵データベース211、及び機密ファイル名変更部212を備えている。

【0052】Client-Proxy間通信制御部201は、Client14との通信を制御するモジュールである。機密ファイルリスト及びアクセスポリシー登録部202は、機密ファイル50へのアクセスが許可されているユーザのユーザIDとパスワードの組を管理するテーブル、及び、Webサーバ11上にある機密ファイル50の一覧と各ファイル50へのユーザのアクセス権限を管理するテーブル及びそのテーブルのバージョン情報を保管している。また、Client14からのポリシーバージョン問い合わせに対して、ポリシーのバージョンを比較し、Proxyサーバ20のポリシーバージョンのほうが新しいものであれば、ポリシーデータをClient14に送信する機能を備えている。受信データ解析部204は、Client14から受信したデータを解析し、アクセス要求ファイルのURLを調べるモジュールである。要求ファイルアクセス判定部203は、受信データ解析部304で獲得したアクセス要求ファイルのURLと機密ファイルリスト及びアクセスポリシー登録部202に登録された機密ファイルのURLリストから、アクセス要求ファイルが機密ファイル50かどうか判断するものであり、機密ファイル50へのアクセスならば、ユーザ認証部205はClient14のポリシー管理モジュール64内のユーザ・Clientマシン認証部642（図13）に、ユーザ情報を入力するためのダイアログボックスをClient14のディスプレイに表示する要求を送信し、ユーザにより入力されたユーザIDとパスワードを受信し、そのユーザ情報をもとにユーザ認証を行なう。ユーザ認証の結果をもとに、要求ファイルアクセス判定部203は機密ファイル50へのアクセスを許可するかどうか決定する。機密ファイル50へのアクセスが許可されたならば、要求ファイルアクセス判定部203は、Webサーバ11に対し機密ファイル50をダウンロードする要求を出す。

【0053】Client14の2次記憶装置67に保存されている暗号化機密ファイル50にアクセスする際に、Client14にあるポリシ管理モジュール64はProxyサーバ20にポリシバージョンの問い合わせを行なうが、Proxyサーバ20のユーザ認証部205は、ポリシ管理モジュール64からのポリシバージョンの問い合わせによる通信の際に、ポリシ管理モジュール64から送信されたユーザIDとパスワードをもとにユーザ認証を行う。

【0054】暗号用共通鍵データベース211は、Webサーバ11上の機密ファイル50にアクセスできるユーザごとに用意された、ユーザ固有の暗号用共通鍵を保管している。暗号用共通鍵選択部206は、ユーザ認証後にユーザに対応する暗号用共通鍵を、暗号用共通鍵データベース211から検索して取り出し、機密ファイル暗号部207に渡す。機密ファイル暗号部207は、Webサーバ11からダウンロードしてきた機密ファイル50をファイル名ごと、アクセスしてきたユーザに固有の暗号用共通鍵を用いて暗号化するモジュールである。機密ファイル名変更部212は、機密ファイル暗号部207で暗号化されたファイルにファイル名を付け、機密ファイルキャッシュ部209に送る。機密ファイルキャッシュ部209は、暗号化された機密ファイル50を一時的にキャッシュしておくところであり、認証されたユーザからアクセスがあればそのファイルをアクセス要求元のClient14に送信する。Web-Proxy間通信制御部208は、Proxyサーバ20とWebサーバ11間の通信を制御するモジュールである。

【0055】図13は、本実施形態におけるClient14内のポリシ管理モジュール64のブロック構成図である。ポリシ管理モジュール64は、通信制御部641、ユーザ・Clientマシン認証部642、ポリシ管理モジュール内復号用共通鍵キャッシュ部643、復号用共通鍵ポリシ判定部644、Viewer-ポリシ管理モジュール間通信制御部645、ポリシ暗号・復号化部646、ポリシキャッシュ部647、認証用ハードウェア固有情報648から構成される。

【0056】通信制御部641は、ポリシ管理モジュール64とネットワーク側通信制御部66との間の通信を制御するモジュールである。ユーザ・Clientマシン認証部642は、ポリシ適用の際に必要なユーザ及びClientマシンの認証を行い、ユーザ情報をキャッシュする。Clientマシン認証の際には、マシンのハードウェア固有情報65を参照し、認証用ハードウェア固有情報648と照合する。ポリシ管理モジュール内復号用共通鍵キャッシュ部643は、復号用共通鍵データベース62からユーザIDをもとに検索したユーザ固有の復号用共通鍵を一時的にキャッシュする。ポリシ暗号・復号化部646では、ポリシデータベース63から読み込まれた暗号化されたポリシデータの復号する。また、Proxyサーバ20から送信された新たに更新すべきポリシデータを暗号

化し、ポリシデータベース63に保存する。

【0057】ポリシキャッシュ部647は、ポリシデータを一時的にキャッシュしておくモジュールである。復号用共通鍵ポリシ判定部644は、ユーザ・Clientマシン認証部642にキャッシュされたユーザ情報とポリシキャッシュ部647にキャッシュされたポリシデータをもとに復号用共通鍵をViewer60に送信するかどうか判定する。

【0058】図21は機密ファイルリスト及びアクセスポリシ管理部に保管されたアクセスポリシデータテーブルの構成図である。テーブル21Aは、Webサーバ11に格納されている機密ファイルのURL2101と、各機密ファイルごとにアクセス可能なユーザの識別番号2102およびこのテーブル21Aのポリシバージョン2103を設定したものである。またテーブル21Bは、機密ファイルにアクセス可能なユーザのユーザID2105とパスワード2106および割り振られた識別番号2104をリストアップしたものである。

【0059】次に、フローチャートを用いて本実施形態における各モジュール間の処理の流れや関連を説明する。図14は、Proxyサーバ20における処理のフローチャートを示したものである。Proxyサーバ20は、Client14からアクセス要求を受信すると（ステップ1400）、Proxyサーバ初期ルーチンに移る（ステップ1401）。このルーチンは、Client14がWebサーバ11上の機密ファイル50または非機密ファイル51にアクセスする為にProxyサーバ20にアクセスしているのか、ポリシ管理モジュール64より、ポリシバージョン問い合わせの為にProxyサーバ20にアクセスしているのかを判定するルーチンである。このProxyサーバ初期ルーチン（ステップ1401）については図16により後述する。

【0060】このルーチンでWebサーバ11上の機密ファイル50または非機密ファイル51へのアクセスであると判定されると、処理は図14のステップ1402に移り、Proxyサーバ20は受信データ解析部204でアクセス要求ファイルのURLを調べる。その後、要求ファイルアクセス判定部203で機密ファイル50へのアクセスであるかどうかの判定が行われる（ステップ1403）。機密ファイル50へのアクセスでなければ、要求ファイルアクセス判定部203は、Webサーバ11からアクセス要求ファイルをダウンロードし（ステップ1404）、ダウンロードしたファイルに何も処理を施さずにアクセス要求元のClient14に送信する（ステップ1405）。

【0061】Client14のアクセス要求ファイルが機密ファイル50であった場合、Proxyサーバ20は、Client14のポリシ管理モジュール64と通信し、アクセス要求を出しているユーザのユーザIDとパスワードを取得する。そして、取得したユーザ情報（ユーザIDとパ

10

20

30

40

50

スワード)と、機密ファイルリスト及びアクセスポリシー登録部202に登録されているユーザ情報と比較照合することにより、ユーザ認証部205でユーザの認証を行なう(ステップ1406)。この認証の結果、正当なアクセス権限を有するユーザであると認証されなかった場合は、機密ファイル50へのアクセスを拒否する(ステップ1409)。しかし、認証された場合は、ユーザ固有の鍵を暗号用共通鍵データベース211から選択し(ステップ1407)、Webサーバ11から機密ファイル50をダウンロードしたあと(ステップ1408)、機密ファイル暗号部207で、その鍵を用いて機密ファイル50をファイル名ごとユーザ固有の暗号用共通鍵で暗号化する(ステップ1410)。なお、暗号用共通鍵データベース211にユーザ固有の暗号用共通鍵を登録する方法としては、ユーザが機密ファイル閲覧のためにClient14及びProxyサーバ20にユーザ登録するときに、Proxyサーバ20と通信して鍵をClient14とProxyサーバ20の両方に作成する方式を採用する。

【0062】Proxyサーバ20はポリシー管理モジュール64と通信し、ポリシー管理モジュール64のユーザ・Clientマシン認証部642にユーザIDとパスワードの入力を促すためのダイアログボックスを表示させ、ポリシー管理モジュール64からProxyサーバ20に送信されたユーザIDとパスワードをもとに、Proxyサーバ20でユーザ認証を行なう。

【0063】暗号化された機密ファイル50は、機密ファイル名変更部212においてファイル名が変更され(ステップ1411)、機密ファイルキャッシュ部209にキャッシュされる。その後、機密ファイルURL送信部210は、変更したファイル名をもとに、そのファイルをProxyサーバ20からダウンロードするためのURLを生成してClient14に送信する(ステップ1412)。そのURLを受けて、Browser61は機密ファイル50をProxyサーバ20からダウンロードする(ステップ1413)。

【0064】図16はProxyサーバ20初期ルーチン(図14のステップ1401)のフローチャートを示したものである。Client14からのアクセスがポリシー管理モジュール64からのポリシーバージョン問い合わせのアクセスであるかどうか判定する(ステップ1601)。この判定法としては、例えば問い合わせのアクセスの際には、Proxyサーバ20に送信するデータのヘッダに、明示的に特定のビット列を挿入し、このビット列を検出する方法等がある。このアクセスがポリシーバージョン問い合わせのアクセスでなかった場合、Webサーバ11へのアクセス要求であるので、図14のProxyサーバ処理のステップ1402に戻る(ステップ1605)。

【0065】ポリシーバージョン問い合わせのアクセスであった場合、問い合わせのアクセスの際にClient14より送信されてきたClient14内のポリシーデータのバージョン

ョンデータを用いて、問い合わせ元のClient14のポリシーバージョンとProxyサーバ20のポリシーバージョンを比較する(ステップ1602)。ポリシーバージョンが等しかった場合、ポリシー管理モジュール64にポリシーのバージョンが等しいことを通知し(ステップ1606)、処理を終了する。ポリシーバージョンが等しくなかった場合、Client14のポリシーデータベース63を更新する必要があるため、Proxyサーバ20のポリシーデータをポリシー管理モジュール64に送信する(ステップ1604)。

【0066】これにより、ポリシーデータベース63内のポリシーデータ、すなわちアクセス権限を判定するためのデータはProxyサーバ20内で管理されている最新のものに更新される。

【0067】図17は、Webサーバ11上のファイルを参照するときのClient14における処理のフローチャートを示したものである。Client14がProxyサーバ20から送信されたファイルを受信すると(ステップ1701)、Browser61はファイル名を参照し、機密ファイル50が受信されたかどうかを判定する(ステップ1702)。機密ファイル50が受信されていない場合、Browser61はそのファイルを自身の表示機能を用いて表示する(ステップ1708)。しかし、受信されてきたファイルが機密ファイル50であった場合、Browser61はViewer60を起動する(ステップ1703)。Viewer60はViewer起動判定部6011でハードウェア固有情報65を調べ(ステップ1704)、Viewer内認証用ハードウェア固有情報6012と照合し、Viewer60が特定のClient14にインストールされていることを確認する。Viewer60に登録されたViewer内認証用ハードウェア固有情報6012と、実際に読み込んだハードウェア固有情報65が一致しなければ、不正にViewer60がコピーされてインストールされているものと判断して、Viewer60を終了する(ステップ1709)。一致した場合は、Browser61からViewer60に、機密ファイル50のデータが転送され(ステップ1706)、暗号化された機密ファイル50は暗号化機密ファイルキャッシュ部6013にキャッシュされる(ステップ1707)。その後、機密ファイル名データ除去部6014にてファイル名の除去が行われ(ステップ1710)、暗号化機密ファイル復号部6015で復号された後(ステップ1711)、機密ファイル表示部6016に復号された機密ファイル50が表示される(ステップ1712)。

【0068】Webサーバ11にある機密ファイル50をダウンロードする際、Proxyサーバ20におけるユーザ認証のために、ポリシー管理モジュール64がダイアログボックスを生成し、ユーザにユーザIDとパスワードの入力を要求するが、その入力値をもとに、ポリシー管理モジュール64はClient14にある共通鍵データベース62より、対応するユーザ固有の共通鍵を検索し、それを

Viewer60のViewer内復号用共通鍵キャッシュ部6017に転送する。ステップ711で復号に使用される共通鍵は、この共通鍵キャッシュ部6017にキャッシュされた共通鍵である。

【0069】図19は、2次記憶装置67に保存された機密ファイル50を参照するときのClient14における処理を示したフローチャートである。ユーザが2次記憶装置67に保存された機密ファイル50にアクセスしたとき、まずViewer60が起動される（ステップ1901）。Viewer60はポリシー管理モジュール64を起動し、10 アクセスしようとしている機密ファイル名をポリシー管理モジュール64に送信する（ステップ1902）。ポリシー管理モジュール64はユーザ・Clientマシン認証部642にてユーザIDとパスワードの入力をユーザに要求し、同時にClientマシンのハードウェア固有情報65にアクセスして、認証用ハードウェア固有情報648を用いてマシン認証を行なう（ステップ1903）。

【0070】ポリシー管理モジュール64は、Proxyサーバ20にユーザIDとパスワード、及びClient14のポリシーのバージョンデータを安全な方法で送信し、ポリシーバージョンの問い合わせをする。そして、ポリシー管理モジュール64は、Proxyサーバ20でのユーザ・Clientマシン認証の結果及びポリシーバージョン問い合わせに対する応答を待つ（ステップ1904）。Proxyサーバ20におけるユーザ・Client認証が否定されたか、もしくは通信の失敗が原因でProxyサーバ20からの応答がなかった場合、ポリシー管理モジュール64はViewer60に20 応答なしの通知を行なう（ステップ1909）。これにより、Viewer60は機密ファイル50を表示しない（ステップ1910）。

【0071】Proxyサーバ20からの応答があり、かつその応答の内容としてポリシーバージョンが等しくなかった場合には、Proxyサーバ20から最新のポリシーデータが送信され、そのデータをもとにポリシーデータベース63を更新する（ステップ1906、1907）。バージョンが等しければ、Client14のポリシーデータはそのままにしておく。復号用共通鍵ポリシー判定部644は、バージョンが最新のポリシーデータを用いて、ユーザIDとアクセス対象の機密ファイル名から機密ファイル50へのアクセスが可能かどうか判定する（ステップ1908、1911）。判定結果が不可の場合、復号用共通鍵ポリシー判定部644はViewer60に機密ファイル50へのアクセス拒否エラーを返す（ステップ1915）。そのエラーを受けて、Viewer60は暗号化された機密ファイル50の復号処理行なわずにエラーを機密ファイル表示部6016に表示し、処理を終了する（ステップ1916）。

【0072】また、ポリシー判定結果が可の場合、復号用共通鍵ポリシー判定部644は、ユーザに固有の復号用共通鍵を復号用共通鍵データベース62から検索し、その

復号用共通鍵をViewer60に送信する（ステップ1912）。Viewer60はファイル名を削除の後、ユーザ固有の復号用共通鍵を用いて機密ファイル50を復号し（ステップ1913）、そのデータをViewer60の機密ファイル表示部6016で表示する（ステップ1914）。

【0073】以上のように、この第2の実施形態の情報提供システムは、Webサーバ11とClient14との間にProxyサーバ20を介在させ、このProxyサーバ20において、Client14からWebサーバ11上の機密ファイル50へのアクセス要求にしたがって、Client14内のポリシー管理モジュール64と通信してユーザ及びClientマシンの認証を行い、予め登録されたユーザからのアクセス要求であった場合には、要求された機密ファイル50をWebサーバ11からダウンロードし、その機密ファイル50を要求元のユーザに対応した暗号化のための共通鍵を用いてファイル名ごと暗号化し、ファイル名を変更し、その変更された機密ファイルをClient14に転送するように構成したものである。

【0074】これにより、既存のWebサーバ11の設定を変更することなく、機密ファイル50に対しユーザごとのアクセス権を設定でき、その機密ファイル50を安全にダウンロードできると共に、その機密ファイル50をClient14内に安全に保管することができる。また、ユーザごとに機密ファイル50へのアクセス権を設定しているので、機密ファイル50のダウンロードの際に盗聴されても、機密ファイル50へのアクセス権のないユーザはそれを閲覧することができない。また、それぞれの機密ファイル50のアクセス権の認証は動的に適用され、Proxyサーバ20でアクセス権を変更した場合、その変更時点から、アクセス権はClient14内に保存してある機密ファイル50にも適用される。従って、例えば人事部に属していたClient14のユーザAが人事異動により、営業部に配置転換された場合には、Proxyサーバ20内の人事部員以外には機密である人事情報ファイルのアクセス権リストからユーザAを削除することにより、ユーザAが使用しているClient14内のポリシーデータベース63に対してもその変更内容が図16のステップ1601～1604の処理で反映され、ユーザAは人事異動前と同じClient14マシンを使用していたとしても機密の人事情報の閲覧は不可能になる。さらに、機密ファイル50を予め暗号化して、Webサーバ11に登録しておく必要がないので、Webサーバ11で動的に生成される機密ファイル50の管理も可能である。

【0075】また、Client14においては、機密ファイル50を表示するために専用にしたViewer60が不正にインストールされたものである場合には、このViewer60を閉じ、機密ファイルを表示させないようにしているため、不正インストールなどの不正行為に対しても有効に対処し、機密ファイル50の漏洩を防止することが

できる。

【0076】また、2次記憶装置67に保管された機密ファイル50にアクセスする場合には、Proxyサーバ20にその都度アクセス権限のバージョンを問い合わせ、最新のアクセス権限判定用の情報でアクセス権限を認証しているため、2次記憶装置67に保管された機密ファイル50を、アクセス権限を取り消された者による不正アクセス行為から防衛することができる。なお、アクセス権限のバージョン問い合わせ処理は、2次記憶装置67をアクセスする都度行なっているが、機密ファイル50の機密度が低いものである場合には所定時間間隔おきにするなど、問い合わせ回数を少なくするようにしてもよい。これにより、ネットワークのトラフィックを少なくすることに貢献することができる。

【0077】なお、第2の実施形態においては、ハードコピー禁止モジュールを設けていないが、第1の実施形態と同様に設けることができる。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵は、Client14の装置自身に固有の情報（MACアドレス、IPアドレス、CPU製造番号など）を元に生成した鍵情報、またはユーザ自身の機密情報（例えばクレジット番号など）から生成した鍵情報を用いてもよい。

【0078】次に、本発明の第3の実施形態を詳細に説明する。図22は、本発明の第3の実施形態を示す全体構成図である。この実施形態のシステムは、地図データや写真等の画像データ、新聞・雑誌の記事といったコンテンツ2207を保管するWebサーバであるコンテンツサーバ2202と、利用者のユーザIDやパスワードを用いたアクセス認証、アクセスログの管理、及びコンテンツ配信時にコンテンツデータが盗まれないように暗号化処理を施すコンテンツ配信プロキシ2203、及びコンテンツを閲覧するための専用ビューア2206a～2206nをそれぞれインストールしたクライアント2205a～2205nから構成されている。コンテンツ配信会社2201はコンテンツサーバ2202、及びコンテンツ配信プロキシ2203を管理し、アクセスログを集計して、利用者にダウンロードしたコンテンツに対する料金を請求する。コンテンツ配信を希望する利用者はインターネット2204経由で専用ビューア2206a～2206nを用いてコンテンツ2207をダウンロードする。コンテンツサーバ2202にアクセスするためには、必ずコンテンツ配信プロキシ2203を経由しなければならない。従って、外部からコンテンツサーバ2202への直接的な不正アクセスを防ぐことができる。

【0079】次に、本発明の第3の実施形態における各構成要素の内部構成、ならびに各構成要素とその構成要素間の処理について説明する。図23は、本発明の第3の実施形態におけるクライアント構成図である。クライアント2205（2205a～2205n）は、専用ビューア2206、ユーザ固有鍵DB22051、クライ

アント固有データ22053、及び2次記憶装置22052から成る。クライアント固有データ22053として、ICカード内の改竄不可能なデータや特別なハードウェア内のデータ、CPUに割り当てられたデータ等を用いることができる。

【0080】専用ビューア2206の詳細な説明をする。専用ビューア2206は表示部22066、ハードコピー禁止モジュール22067、復号部22063、復号データキャッシュ部22064、暗号・復号化部22065、鍵検索部22061、及び鍵生成部22062から成る。表示部22066はコンテンツを展開して表示する部分である。復号部22063はコンテンツ配信プロキシ2203から送信された暗号化されたコンテンツを、鍵検索部22061でユーザ固有鍵DB22051から検索されたユーザ固有の鍵で復号する部分である。鍵生成部22062は、専用ビューア2206の起動時に読み込んだクライアント固有データ22053を元に、コンテンツ保存時に暗号化・復号化するためのクライアント固有の鍵を生成する。鍵検索部22061は、ユーザID・パスワード情報を元に、ユーザ固有鍵DB22051から検索してユーザ固有の鍵を抽出する。ユーザID・パスワード情報は、専用ビューア2206に予め登録する、もしくは専用ビューア2206を用いてコンテンツ配信プロキシ2203へアクセスする際や2次記憶装置22052内に保存された暗号化されたコンテンツにアクセスする際にダイアログを表示して、利用者に入力させるなどの方法で取得する。ユーザ固有鍵DB22051は、各利用者固有の鍵を管理する部分であり、利用者の鍵は利用者のパスワードを鍵として用いて暗号化する等の処置を施してクライアント2205内に安全に保管される。ICカードや別のハードウェア等に保存する方法でもよい。

【0081】暗号・復号化部22065は鍵生成部22062、及び鍵検索部22061からそれぞれ、クライアント固有の鍵及び利用者固有の鍵を受け取り、その2つの鍵を用いてコンテンツを暗号化、もしくは復号化する。ハードコピー禁止モジュール22067は、キャプチャツールがハードコピーをする際に使用するOSのシステムコールをフックして禁止すること、及びハードコピーを撮るためのキーを押下した際に発行されるシステム内のメッセージをフックしてデータのコピー先メモリを使用禁止することにより、表示されている画面のハードコピーを禁止するモジュールである。このモジュールにより、利用者がディスプレイ画面にコンテンツを表示し、そのハードコピーを採取して二次配布することを防止する。

【0082】図24は本実施形態におけるコンテンツ配信プロキシ2203の構成図である。コンテンツ配信プロキシ2203はプロキシサーバ22031、管理アプリケーション22032、ユーザ情報・固有鍵DB22



033及びログデータ保存部22034から成る。ユーザ情報・固有鍵DB22033はコンテンツにアクセス可能な利用者のユーザID、パスワード、鍵データ及びアクセス可能なコンテンツのURL情報を格納するデータベースであり、管理アプリケーション22032によりユーザ情報・固有鍵DB22033への設定情報の登録・削除・変更が行われる。プロキシサーバ22031は、クライアント2205のコンテンツサーバ2202へのアクセスを中継して処理するプログラムであり、コンテンツへのアクセスログをログデータ保存部22034に書き込む。

【0083】プロキシサーバ22031の詳細説明に移る。プロキシサーバ22031はコンテンツキャッシュ部22035、ユーザ認証部22036、受信データ解析部22037、及びコンテンツ暗号化部22038から成る。クライアント2205から送信されるアクセス要求は、アクセス要求コンテンツのURL、ユーザID及びパスワードで構成されており、プロキシサーバ22031は受信したアクセス要求を受信データ解析部22037で解析する。受信データ解析部22037で取得したユーザ情報、及びアクセス要求コンテンツのURLを元に、ユーザ情報・固有鍵DB22033を検索し、ユーザ認証、及びコンテンツへのアクセスが可能かどうか判定を行なう。認証が成功すると、コンテンツサーバ2202にクライアント2205からのリクエストを送信し、ダウンロードしたコンテンツデータを、ユーザ情報・固有鍵DB22033から検索した利用者固有の鍵で暗号化してクライアント2205に送信する。

【0084】図25は本実施形態におけるコンテンツ配信プロキシ2203で保存されるコンテンツアクセスログデータの概要構成図である。これはコンテンツ配信プロキシ2203のログデータ保存部22034に記録されるデータエントリであり、トランザクション番号2501、ユーザID2502、アクセス日時2503、アクセスコンテンツURL2504、課金フラグ2505で構成されている。トランザクション番号2501はテーブルのキーとなる値で、クライアント2205からコンテンツ2207へのアクセスごとに割り振られる。アクセスコンテンツURL2504は、利用者がアクセスしたコンテンツ2207のURLである。課金フラグ2505は、そのトランザクションに対して課金するかどうかを示すフラグで、例えば同じ利用者による同一コンテンツの2回目以降のアクセスに対しては課金しないサービスの場合等に利用する。

【0085】図26は本実施形態におけるユーザ情報・固有鍵DB22033に記録されたアクセス可能な利用者のユーザ情報を示す概要構成図である。このテーブルの各エントリはユーザID2601、パスワード2602、サービス登録日2603、サービス利用期限日2604、固有鍵データ2605、及びアクセス可能コン

テンツURL2606で構成されている。サービス登録日2603は、利用者がWeb経由でコンテンツ配信サービスに登録した日付であり、サービス利用期限日2604は、利用者の配信サービス授受可能な期日を表す。固有鍵データ2605はユーザに固有の鍵データを登録しておく項目である。また、アクセス可能コンテンツURL2606はユーザがアクセス可能なコンテンツのURLのリスト2607へのポインタが登録されており、利用者により選択された配信サービスを受けたいコンテンツに対応している。上記のエントリは登録された利用者ごとに用意されており、コンテンツ配信プロキシ2203の管理アプリケーション22032で登録・削除・変更を行なう。

【0086】図27は、本実施形態におけるコンテンツ配信サービスにおける全体の流れを時系列で示した図である。この図に従って、利用者のコンテンツ配信サービス依頼からサービスの処理、サービス料金の支払いまでの一連の流れについて説明する。利用者はコンテンツ配信会社2201のコンテンツ配信サービスのサイトにアクセスして、コンテンツの表示に必要な専用ビューア2206をダウンロードしてクライアント2205にインストールする(ステップ2701)。利用者は専用ビューア2206を用いてWeb経由でコンテンツ配信を依頼する(ステップ2702)。コンテンツ配信会社2201のコンテンツ配信プロキシ2203の管理アプリケーション22032は、利用者のユーザID、パスワード、アクセス可能なコンテンツURL等の設定情報をユーザ情報・固有鍵DB22033に登録する(ステップ2703)。また、この際に生成されるコンテンツ配信の際に使用するユーザに固有の鍵データもユーザ情報・固有鍵DB22033の固有鍵データエントリ2605に登録する。そして、この登録した固有鍵を利用者に通信を暗号化するなど、安全な方法で配信する(ステップ2704)。

【0087】次に配信サービスが行われるが、その流れについて説明する。まず、利用者は専用ビューア2206を用いてコンテンツ2207にアクセスする(ステップ2705)。コンテンツ配信会社2201はコンテンツ2207へのアクセスに対してアクセスログを採取することで利用者に対する課金処理を行なう(ステップ2706)。そして、アクセス要求されたコンテンツを利用者に配信する(ステップ2707)。この流れを利用者のコンテンツ2207へのアクセスごとに繰り返す。最後に、コンテンツ配信会社2201は予め定められた期間末に、利用者ごとに決済を行い(ステップ2708)、クレジットカード会社経由で利用者にコンテンツ使用料を請求する(ステップ2709)。利用者は請求に応じてコンテンツ使用料の支払いを行なう(ステップ2710)。

【0088】図28は、コンテンツ2207をダウンロ

ードして専用ビューア2206で閲覧する際のフローチャートである。以下、フローチャートに従って処理の流れを説明する。利用者は、クライアント2205にインストールされた専用ビューア2206を使用して、コンテンツ配信プロキシ2203にアクセスする(ステップ2801)。アクセスの方法として、利用者は専用ビューア2206のインターフェイス(後述の図30参照)にあるコンテンツのURLを入力するエディットボックス3001に、閲覧したいコンテンツのURLを入力してアクセス要求を送信する。コンテンツのURLを送信する際に、専用ビューア2206に予め登録されているか、もしくはダイアログボックスを表示してユーザにより入力されたユーザIDとパスワードも、コンテンツURLと共にコンテンツ配信プロキシ2203に送信する(ステップ2802)。

【0089】コンテンツ配信プロキシ2203は専用ビューア2206から送信されたリクエストを解析して、送信されたユーザID、パスワード、及びコンテンツのURLを元にユーザ情報・固有鍵DB22033に検索をかけ、ユーザ認証、及びコンテンツアクセス許可判定を行なう(ステップ2803)。認証・アクセス許可判定が成功しない場合、プロキシサーバ22031はクライアント2205にコンテンツ利用不可を表示するデータを送信し(ステップ2806)、処理を終了する。成功した場合、プロキシサーバ22031はコンテンツサーバ2202からコンテンツをダウンロードして、ユーザ情報・固有鍵DB22033に登録された固有鍵を使用して暗号化を行い(ステップ2804)、要求元のクライアント2205の専用ビューア2206に送信する。専用ビューア2206は、暗号化されたコンテンツを、ユーザ固有鍵DB22051で検索した固有鍵を使用して復号表示する(ステップ2805)。

【0090】図29はクライアント2205にコンテンツデータを保存する際の、専用ビューアが行なう処理のフローチャートを示したものである。以下、このフローチャートに従って、処理の流れを詳細に説明する。専用ビューア2206は起動時にクライアント固有データ22053をアプリケーション内に取得する(ステップ2901)。そして、取得したクライアント固有データ22053を元に、鍵生成部22062においてクライアント固有の鍵を生成する(ステップ2902)。次に、専用ビューア2206は、コンテンツをダウンロードする際に使用するためのユーザIDとパスワードを、ダイアログボックスを表示して利用者に入力してもらうか、もしくは予め専用ビューア2206に登録されているのであればそれを読み取る(ステップ2903)。そして、受け取ったユーザ情報をもとに、専用ビューア2206内の鍵検索部22061において、利用者固有の鍵を検索して抽出する(ステップ2904)。この生成・抽出された2つの鍵を利用して、専用ビューア2206

内の暗号・復号化部22065においてコンテンツデータを暗号化する(ステップ2905)。最後に、暗号化したコンテンツデータを2次記憶装置22052に保存する(ステップ2906)。2次記憶装置22052に保存されたコンテンツデータを復号表示する際にも、同様の手順で行なう。このように、コンテンツを暗号・復号化するための2つの鍵が、それぞれクライアント2205、及び利用者に固有であるため、もし、保存されたコンテンツデータを、専用ビューア2206のインストールされた他のクライアントにコピーして表示しようとしてもできない。従って、配信されたコンテンツのアクセス権を保持する利用者による2次配信を防ぐことができる。

【0091】図31は、専用ビューア2206を使用してデジタルコンテンツ配信サービスに登録する際のインターフェイスの移り変わりを表した図である。利用者は、まずコンテンツ配信会社2208のサイトからダウンロードしてきた専用ビューア2206を使用し、デジタルコンテンツ配信登録ページ3101にアクセスする。デジタルコンテンツ配信登録ページ3101は、氏名、性別、住所、メールアドレス、クレジットカード番号等の個人情報、配信サービスで利用する利用者希望のユーザID・パスワード、及び配信サービスを受けたいコンテンツ項目を入力するフォームで構成されている。利用者はこれらのフォームに記入して「OK」ボタンを押す。また、フォームの入力を白紙に戻したい場合は「取消」ボタンを押す。「OK」ボタンを押すと、入力情報確認のページ3102が表示される。このページ3102で、利用者は先に入力した情報を確認する。入力情報が正しければ「送信」ボタンを押す。入力情報が正しくない、もしくはコンテンツ配信サービスの登録を中止する場合には、それぞれ「戻る」もしくは「中止」ボタンを押す。「送信」ボタンを押すと、入力情報がコンテンツ配信プロキシ2203に送信される。そして、管理アプリケーション22032により利用者に固有の鍵が生成され、ユーザIDやパスワード、ユーザ情報と共にユーザ情報・固有鍵DB22033に登録される。その後、固有鍵データがコンテンツ配信プロキシ2203よりクライアント2205内の専用ビューア2206に送信される。その際、図32に示すようにデータの送信状況を示す画面3103がクライアント2205に表示される。利用者の固有鍵の送信が完了すると、図32に示す登録完了ページ3104が表示される。このページ3104には登録された利用者のユーザID情報が表示される。パスワード情報はメールにより別途利用者に送信される。これにより、利用者は登録されたパスワード情報の確認も行なう。

【0092】図33は本発明の第4の実施形態を示した全体構成図である。コンテンツ配信サービスは、クライアント3303、コンテンツ配信会社3301、クレジ

ットカード会社3302の3者間で行われる。コンテンツ配信会社3301はコンテンツ3306と、コンテンツ3306を格納するWebサーバであるコンテンツサーバ3305を管理している。また、コンテンツ配信プロキシ3307はクレジットカード会社3302で管理されており、クライアント3303には専用ビューア3308がインストールされている。各関係者はインターネット3304経由でそれぞれ通信を行なう。コンテンツサーバ3305にはコンテンツ配信プロキシ3307しかアクセスできず、かつ通信は安全なものとする。例えば両者を専用線で接続、あるいはSSLクライアント認証通信等の方法でコンテンツサーバ3305はコンテンツ配信プロキシ3307を認証したうえで通信を行なう。本実施形態ではコンテンツサーバ3305とコンテンツ配信プロキシ3307はSSLクライアント認証方式で通信を行なうものとする。

【0093】図34は本実施形態におけるクライアント3303の構成図を示したものである。クライアント3303は、2次記憶装置3401、クレジットカードデータ3402、専用ビューア3308から成る。クレジットカードデータ3402はクレジットカードの番号情報で、クライアント3303に平文のまま保存されているか、パスワードとして利用者が専用ビューア3308に入力するものとする。専用ビューア3308は、復号データキャッシュ部3403、表示部3404、ハードコピー禁止モジュール3405、暗号・復号化部3406、鍵生成部3407、及びハッシュ生成部3408で構成される。コンテンツ配信プロキシ3307より送信されたコンテンツデータを暗号・復号するための鍵は、ハッシュ生成部3408でクレジットカードデータ3402のハッシュ値を計算し、そのハッシュ値を元に鍵生成部3407で生成され、一時的に格納される。この鍵生成は専用ビューア3308の起動ごとに行われる。鍵生成部3407に格納された鍵は、専用ビューア3308のプロセスが終了する際に消去される。暗号・復号化部3406はキャッシュされた鍵を元にコンテンツデータを暗号・復号化するモジュールである。復号データキャッシュ部3403、表示部3404、及びハードコピー禁止モジュール3405については第1の実施形態と同様の構成および機能である。

【0094】図35は、本実施形態におけるコンテンツ配信プロキシ3307の構成図を示したものである。コンテンツ配信プロキシ3307は、プロキシサーバ3501、管理アプリケーション3502、ユーザ情報・固有鍵DB3503、及びログデータ保存部3504より構成される。ユーザ情報・固有鍵DB3503はコンテンツにアクセス可能な利用者のクレジットカード番号、クレジットカード番号のハッシュ値、利用者固有の鍵データ及びアクセス可能なコンテンツのURL情報を格納するデータベースであり、管理アプリケーション3

502により設定情報の登録・削除・変更が行われる。プロキシサーバ3501はクライアント3303のコンテンツサーバ3305へのアクセスを中継して処理するプログラムであり、コンテンツ3306へのアクセスログをログデータ保存部3504に書き込む。第3の実施形態と違って、本実施形態ではユーザIDとパスワードによるユーザ認証の代わりに、クレジットカードデータのハッシュ値による利用者のユーザ認証を行なう。これは、コンテンツ配信プロキシ3307を管理しているのがクレジットカード会社であるため、クレジットカード番号と利用者を1対1に対応づけることができ、クレジットカード番号による利用者の識別の方が課金処理の際に便利だからである。また、管理アプリケーション3502は利用者ごとにコンテンツを暗号化するための鍵の生成するが、この鍵は専用ビューア3308内で生成する方法と同じ方法、すなわちクレジットカードデータ3402よりハッシュ値を求め、その値を元に鍵を生成する方法で生成される。専用ビューア3308からコンテンツ配信プロキシ3307にユーザ認証のためにクレジットカード番号のハッシュ値を送る際には、このハッシュ値がインターネット3304上で盗まれないように暗号化処理を行っておく必要がある。

【0095】次に、プロキシサーバ3501の詳細説明を行なう。プロキシサーバ3501は、SSL通信制御部3505、ユーザ認証部3506、受信データ解析部3507、コンテンツ暗号化部3508、及び通信制御部3509で構成される。SSL通信制御部3505は、コンテンツサーバ3305とコンテンツ配信プロキシ3307の通信として、SSLによるクライアント認証通信を実現するためのモジュールである。これにより、コンテンツサーバ3305にはコンテンツ配信プロキシ経由でしかアクセスできず、また、通信盗聴者によるコンテンツサーバ3305からコンテンツ配信プロキシ3307への通信時のコンテンツデータの漏洩を防ぐ。受信データ解析部3507、ユーザ認証部3506及びコンテンツ暗号化部3508は第3の実施形態と同様の構成及び機能である。通信制御部3509はプロキシサーバ3501とクライアント3303間の通信を司る部分である。

【0096】図36はコンテンツ配信サービス全体の流れを時系列で表した図である。以下、この図に従ってサービス全体の流れを説明する。コンテンツ配信会社3301は予めクレジットカード会社3302にコンテンツ配信サービスにおける課金処理を依頼し、クレジットカード会社3302とコンテンツ配信会社3301の双方は、課金サービスについての契約を交わす(ステップ3601)。契約が成立すると、クレジットカード会社3302はコンテンツ配信プロキシ3307を設置し、コンテンツ配信サービスを開始する。コンテンツ配信サービスを受けたい利用者は、クレジットカード会社330

2とカード使用契約を行い、クレジットカードを取得する(ステップ3602)。コンテンツ配信サービスを受けるために、利用者はコンテンツ配信会社3301のサイトにアクセスして専用ビューア3308をダウンロードし、専用ビューア3308を使用してコンテンツ配信サービスを実施する(ステップ3603)。そして一定期間ごとに決済を行い(ステップ3604)、コンテンツ料金を利用者に代わってコンテンツ配信会社3301に立て替える(ステップ3605)。そして、クレジットカード会社3302は利用者にコンテンツ料金の請求を行い(ステップ3606)、利用者はその請求に対してコンテンツ料金の支払いを行なう(ステップ3607)。

【0097】図37は、コンテンツ3306をダウンロードして専用ビューア3308で閲覧する際のフローチャートを示している。まず、利用者は専用ビューア3308を使用してコンテンツ配信プロキシ3307にインターネット3304経由でアクセスする(ステップ3701)。コンテンツ配信プロキシ3307との接続が確立した後、専用ビューア3308からコンテンツ配信プロキシ3307にクレジットカード番号のハッシュ値が暗号化されて送信される(ステップ3702)。プロキシサーバ3501でクライアント3303からの送信データを解析し、クレジットカードのハッシュ値を元にユーザ認証部3506にて利用者のユーザ認証、及びアクセス許可判定が行われる(ステップ3703)。ユーザ認証が成功すれば、プロキシサーバ3501はコンテンツサーバ3305との間でSSLクライアント認証接続を行い(ステップ3704)、SSLクライアント認証成功の後、コンテンツサーバ3305からコンテンツ3306をダウンロードして暗号化する(ステップ3705)。暗号化されたコンテンツ3306はクライアント3303に送信され、専用ビューア3308で暗号化されたコンテンツが復号表示される(ステップ3706)。しかし、ユーザ認証が成功しなかった場合には、クライアント3303に利用不可のページを表示する(ステップ3707)。

【0098】図38はクライアント3303にコンテンツデータを保存する際の専用ビューア3308が行なう処理のフローチャートである。専用ビューア3308は起動時にクレジットカードデータ3402を取得する(ステップ3801)。そして、ハッシュ生成部3408においてクレジットカードデータ3402のハッシュ値を計算する(ステップ3802)。さらに、鍵生成部3407においてハッシュ値を元に利用者固有の鍵を生成する(ステップ3803)。そして生成された鍵は鍵生成部3407にて保管される。コンテンツデータを保存する際に、この生成された鍵を元にコンテンツデータの暗号化を行い(ステップ3804)、暗号化されたデータを2次記憶装置3401に保存する(ステップ38

05)。

【0099】本実施形態が、第3の実施形態と異なる特徴点を挙げると次の通りである。まず、専用ビューアがダウンロードしたコンテンツデータを保存するときに、利用者が他の人に公開することのできないクレジットカード番号を元にコンテンツデータを暗号化する点がある。この方法を採用することにより、悪意ある利用者がダウンロードしたコンテンツを第3者に2次配布するためには、自分自身のクレジットカード番号を公開するという危険を負わなければならない。通常はこのような危険を冒すことは考えられないため、結果的に、第3者に2次配布することを抑制することが可能になる。また、第3の実施形態では、ダウンロードして保存したクライアントでしかコンテンツを利用することができないが、本実施形態では利用者が別のマシンに暗号化保存されたデータをコピーして、パスワード入力もしくはコピー先のマシンの所定の場所にクレジットカードデータを書き込むことで利用することができる。

【0100】ところで、上記で説明した第1～第4の実施形態において、コンテンツ提供サーバからクライアントに配信するコンテンツは、専用ビューアに表示する可視データであるものと説明したが、本発明で扱うことができる配信データは、書類、新聞、雑誌、写真、絵画等の静止画、映画やテレビ等の動画データだけでなく、音楽または音声として再生可能なデータ、医療機関で扱うカルテ等の医療情報、公共機関が発行する電子化された書類(住民票、印鑑証明書など)、無人の物品引取り所において保管庫から物品等を受取るロッカー鍵に相当する受け取り票などのデータも含まれるものである。また、機械的な動作として再現するための制御データも含まれる。機械的な動作として再現するデータとしては、例えば介護ロボットに掃除、洗濯などの特定の動作をさせるものが考えられる。従って、専用ビューアは可視化データを表示するディスプレイに限定されるものではなく、音声、音楽を再生出力する装置、あるいは機械的な動きに再現する装置を含むものである。

【0101】また、いずれの実施形態においても、ユーザはコンテンツサーバから直接にコンテンツ配信サービスを受ける例を示したが、地域別に分けられた2次配信サービス業者または機関を経由する構成であってもよい。図39は、その例を示す構成図であり、専用ビューア3907を備えたクライアント3904a～3904nは地域別に分割された中継地点a～nの2次配信サービス機関3902a～3902nにコンテンツ配信要求をインターネット3903を介して行なう。要求を受けた中継地点a～nの2次配信サービス機関3902a～3902nのコンテンツ配信プロキシ3906では、要求されたコンテンツがキャッシュされていれば、それを要求元のクライアントに配信する。キャッシュされていなければ、中継サーバ3905を介してコンテンツ配信

会社3091のコンテンツサーバ3903に要求し、取得したコンテンツを要求元のクライアントに配信する。

【0102】

【発明の効果】以上説明したように、本発明によれば、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置（または端末）のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすることができる。また、閲覧した機密情報を第三者に漏洩しないように要求元装置内に保存・管理することができる。また、デジタルコンテンツに課金して配信するサービスにおいて、利用者に配信されたデジタルコンテンツが2次配信されることを防ぎ、デジタルコンテンツ配信サービスにおける正当な課金の仕組みを維持し、不正コピーによる配信サービス業における経営基盤の崩壊を防ぐことに貢献することができる。

【図面の簡単な説明】

【図1】本発明における情報提供システムの第1の実施形態を示す全体構成図である。

【図2】図1の実施形態におけるProxyサーバのブロック構成図である。

【図3】図1の実施形態における通信フックモジュールブロック構成図である。

【図4】図1の実施形態における外部Viewerのブロック構成図である。

【図5】図1の実施形態におけるProxyサーバの処理を示すフローチャートである。

【図6】図1の実施形態における通信フックモジュールのデータ送信時における処理を示すフローチャートである。

【図7】図1の実施形態における通信フックモジュールのデータ受信時における処理を示すフローチャートである。

【図8】図1の実施形態における2次記憶装置アクセス制御部の機密ファイルアクセス時の処理を示すフローチャートである。

【図9】図1の実施形態における外部Viewerの受信データ表示処理を示すフローチャートである。

【図10】本発明の情報提供システムの第2の実施形態を示す全体構成図である。

【図11】図10の実施形態におけるClientのブロック構成図である。

【図12】図10の実施形態におけるProxyサーバのブロック構成図である。

【図13】図10の実施形態におけるClient内のポリシー管理モジュールのブロック構成図である。

【図14】図10の実施形態におけるProxyサーバの処理を示すフローチャートである。

【図15】図14の続きを示すフローチャートである。

【図16】図10の実施形態におけるProxyサーバの初期ルーチンを示すフローチャートである。

【図17】図10の実施形態におけるWebサーバ上のファイル参照時のClientにおける処理を示すフローチャートである。

【図18】図17の続きを示すフローチャートである。

【図19】図10の実施形態における2次記憶装置に保存された機密ファイル参照時のClientにおける処理を示すフローチャートである。

【図20】図19の続きを示すフローチャートである。

【図21】図10の実施形態における機密ファイルリスト及びアクセスポリシー管理部に保管されたアクセスポリシーデータテーブルの構成図である。

【図22】本発明の第3の実施形態を示す全体構成図である。

【図23】第3の実施形態におけるクライアント構成図である。

【図24】第3の実施形態におけるコンテンツ配信プロキシ構成図である。

【図25】第3の実施形態においてコンテンツ配信プロキシで保存されるコンテンツアクセスログデータの概要構成図である。

【図26】第3の実施形態においてユーザ情報・固有鍵DBに記録されたアクセス可能な利用者のユーザ情報の概要構成図である。

【図27】第3の実施形態においてコンテンツ配信サービスにおける全体の流れを時系列で示した図である。

【図28】第3の実施形態においてコンテンツをダウンロードして専用ビューアで閲覧する際のフローチャートである。

【図29】第3の実施形態においてクライアントにコンテンツデータを保存する際の専用ビューアが行なう処理のフローチャートである。

【図30】第3の実施形態において専用ビューアインターフェイス図である。

【図31】第3の実施形態において専用ビューアを使用してデジタルコンテンツ配信サービスに登録する際のインターフェイスの移り変わりを表した図である。

【図32】図31の続きを示す図である。

【図33】本発明の第4の実施形態を示す全体構成図である。

【図34】第4の実施形態におけるクライアント構成図である。

【図35】第4の実施形態におけるコンテンツ配信プロキシ構成図である。

【図36】第4の実施形態におけるコンテンツ配信サービス全体の流れを時系列で示した図である。

【図37】第4の実施形態においてコンテンツをダウンロードして専用ビューアで閲覧する際のシステム全体の

フローチャートである。

【図38】第4の実施形態においてクライアントにコンテンツデータを保存する際の専用ビューアが行なう処理のフローチャートである。

【図39】中継サーバを介して配信サービスを行なう場合の例を示す全体構成図である。

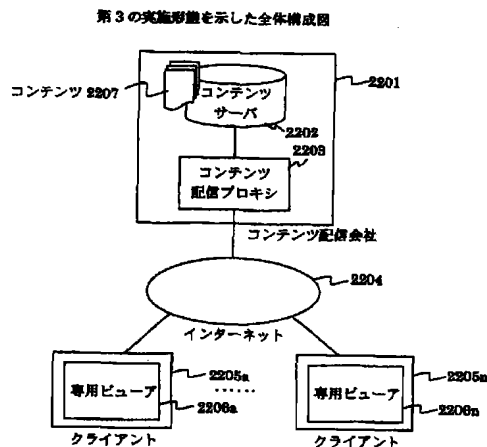
【図40】従来システムの構成図である。

【符号の説明】

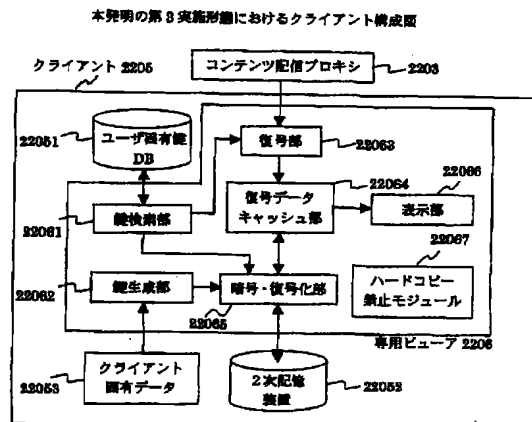
11…Webサーバ、12…ルータ、13…ネットワーク、14…Client、15、61…Browser、16…ハードコピー禁止モジュール、17…2次記憶装置、18…2次記憶装置アクセス制御部、19…アクセストークン、20…Proxyサーバ、22…機密ファイルURL登録部、23…Client14マシン識別子データベース、24…Proxy内受信データ解析部、25…Clientマシン認証部、27…機密ファイル識別子付加部、28…機密ファイル暗号化部、29…共通鍵データベース、30…通信フックモジュール、32…機密ファイル識別子格納部、33…暗号化ファイル復号部、34…共通鍵格納部、35…受信データ解析部、36…送信データ解析部、38…Clientマシン識別子付加部、39…Viewer起動処理部、40…外部Viewer、42…機密ファイル表示部、43…機密ファイルキャッシュ部、44…機密ファイルアクセス・保存処理部、45…ハードコピー禁止モジュール起動処理部、46…2次アクセス制御部起動処理部、47…外部Viewer起動判定部、50…機密ファイル、51…非機密ファイル、60…Viewer、62…復号用共通鍵データベース、65…ハードウェア固有情報、63…ポリシーデータベース、64…ポリシー管理モジュール、6011…Viewer起動判定部、6014…機密ファイル名データ除去部、6015…暗号化機密ファイル復号部、6016…機密ファイル表示部、202…機密フ

\*ファイルリスト及びアクセスポリシー管理部、203…要求ファイルアクセス判定部、205…ユーザ認証部、206…暗号用共通鍵選択部、207…機密ファイル暗号部、210…機密ファイルURL送信部、211…暗号用共通鍵データベース、212…機密ファイル名変更部、644…復号用共通鍵ポリシー判定部、646…ポリシー暗号・復号化部、2201…コンテンツ配信会社、2202…コンテンツサーバ、2203…コンテンツ配信プロキシ、2204…インターネット、2205a～2205n、2205…クライアント、2206、2206a～2206n…専用ビューア、2207…コンテンツ、22051…ユーザ固有鍵DB、22052…2次記憶装置、22053…クライアント固有データ、22061…鍵検索部、22062…鍵生成部、22063…復号部、22065…暗号・復号化部、22067…ハードコピー禁止モジュール、22031…プロキシサーバ、22032…管理アプリケーション、22033…ユーザ情報・固有鍵DB、22034…ログデータ保存部、22036…ユーザ認証部、22037…受信データ解析部、22038…コンテンツ暗号化部、3302…クレジットカード会社、3303…クライアント、3305…コンテンツサーバ、3306…コンテンツ、3307…コンテンツ配信プロキシ、3308…専用ビューア、3401…2次記憶装置、3402…クレジットカードデータ、3405…ハードコピー禁止モジュール、3406…暗号・復号化部、3407…鍵生成部、3408…ハッシュ生成部、3501…プロキシサーバ、3502…管理アプリケーション、3503…ユーザ情報・固有鍵DB、3504…ログデータ保存部、3505…SSL通信制御部、3506…ユーザ認証部、3507…受信データ解析部、3508…コンテンツ暗号化部。

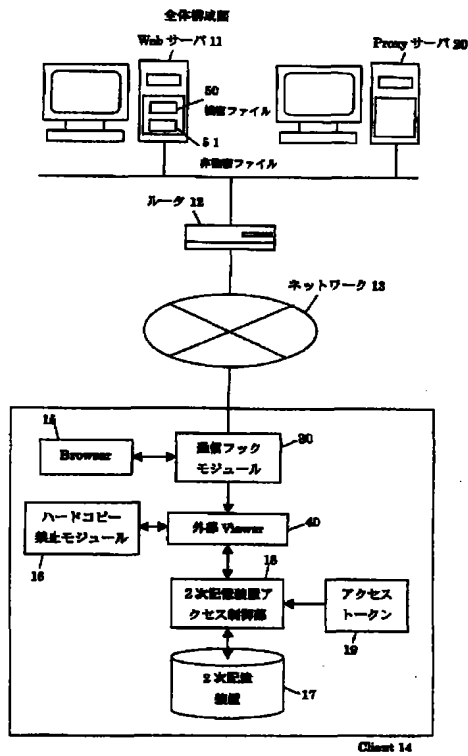
【図22】



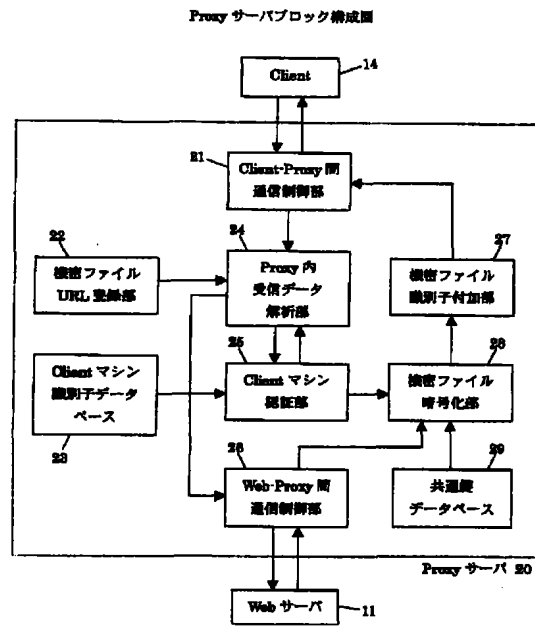
【図23】



【図1】

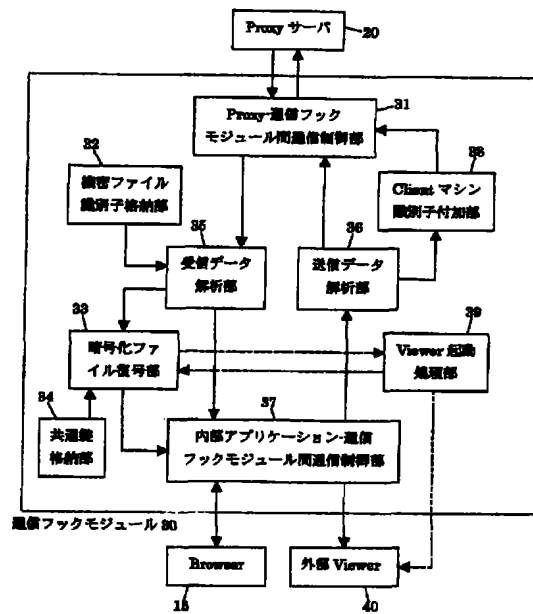


【図2】



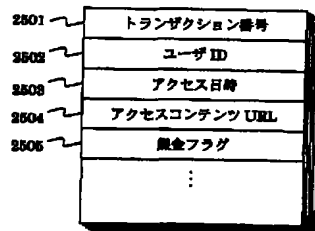
【図3】

通信フックモジュールブロック構成図

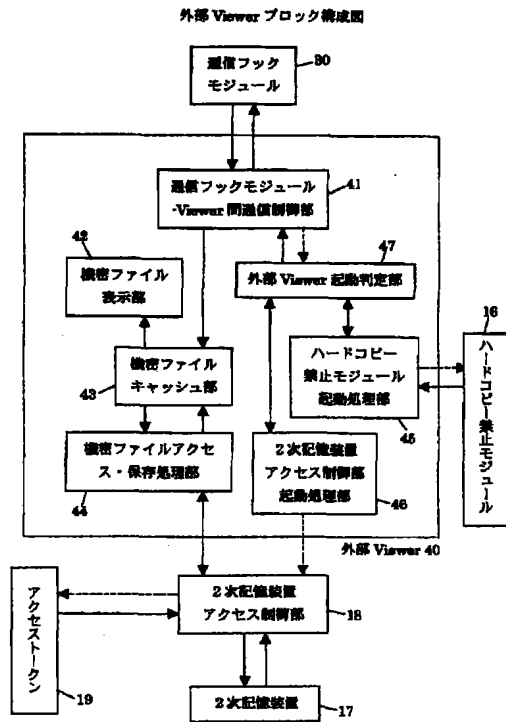


【図25】

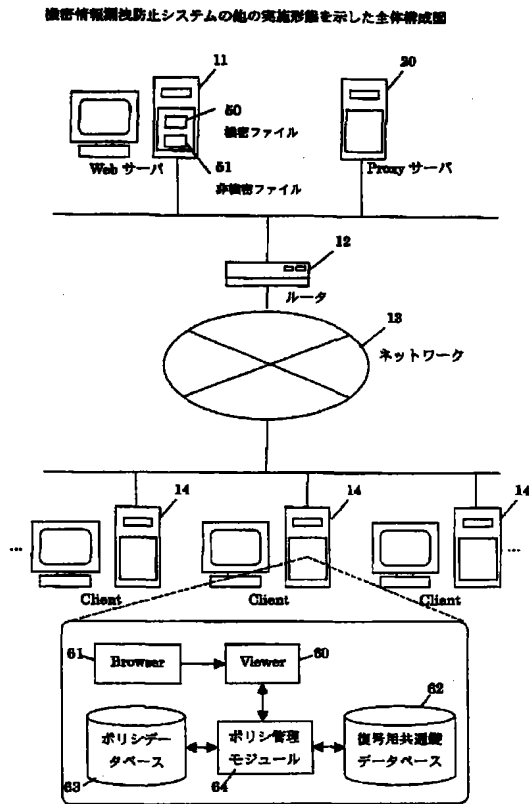
コンテンツ配信プロキシで保存される  
コンテンツアクセスログデータの概要構成図



【図4】



【図10】



【図21】

機密ファイルリスト及びアクセスポリシー管理部に保管された  
アクセスポリシーテーブル図

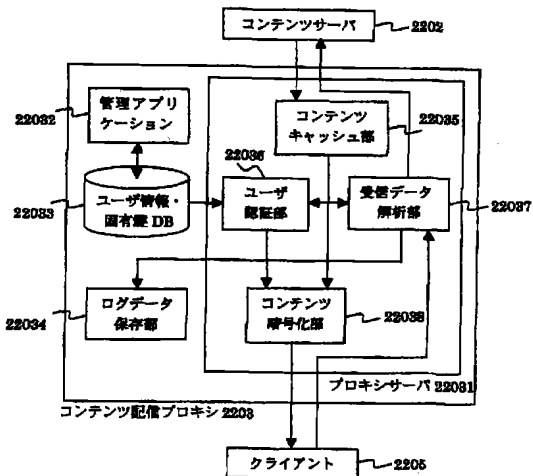
機密ファイル URL	アクセス可能ユーザ	ポリシーバージョン
http://www.secure/secret1.html	001,002,003	2000/1/11/14:30
http://www.secure/secret2.html	004,005	
http://www.secure/secret3.html	003,004,008	
...	...	...

識別番号	ユーザ ID	password
001	user001	*****
002	user002	*****
003	user003	*****
...	...	...

【図24】

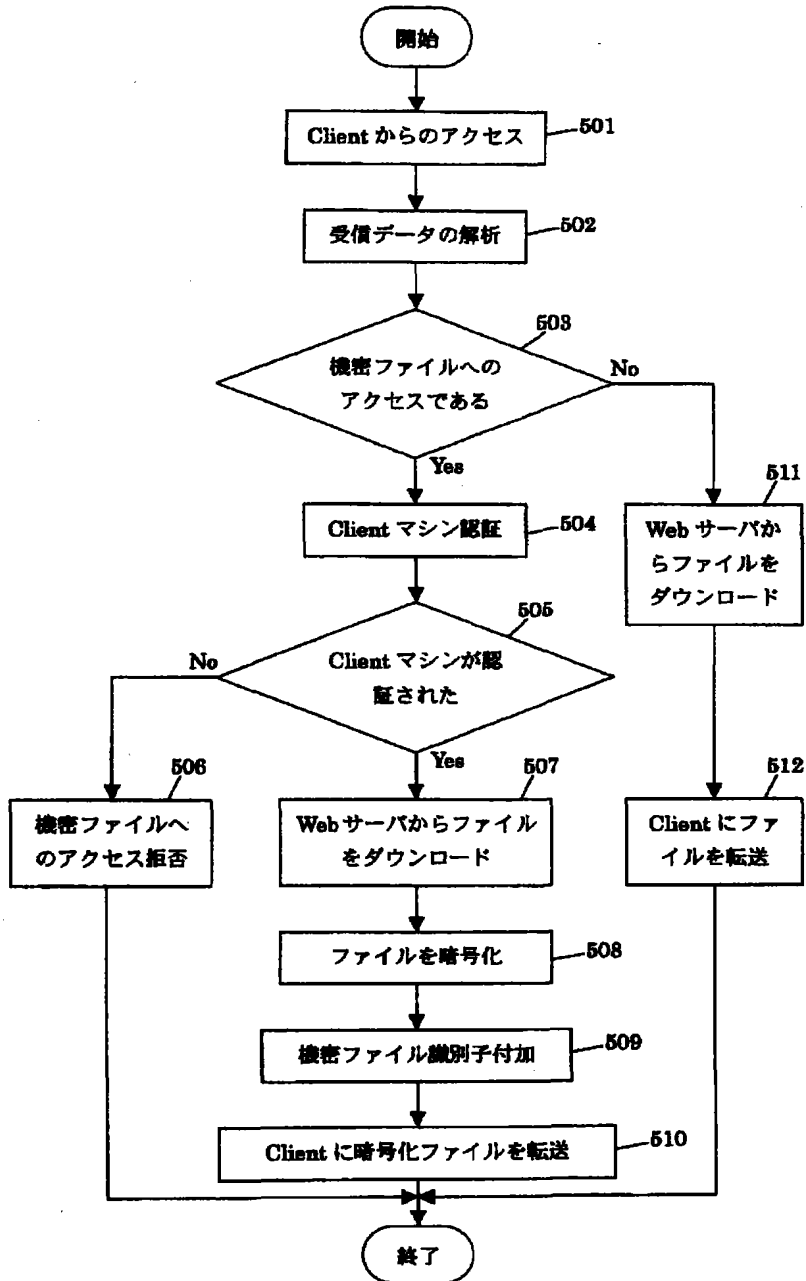
本発明におけるコンテンツ配信プロキシ構成図



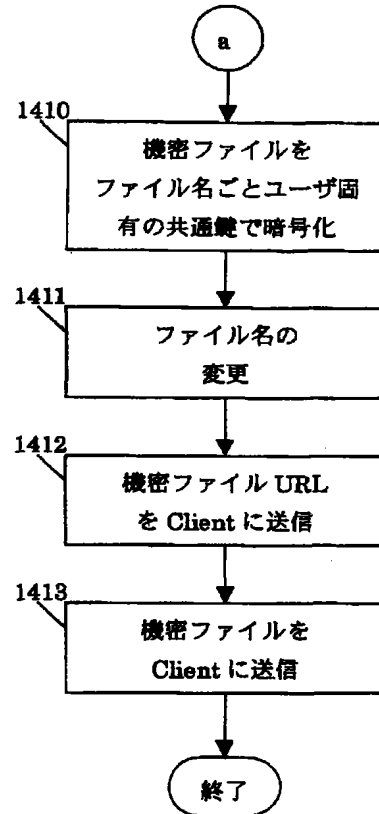


【図5】

Proxy サーバにおける処理のフローチャート

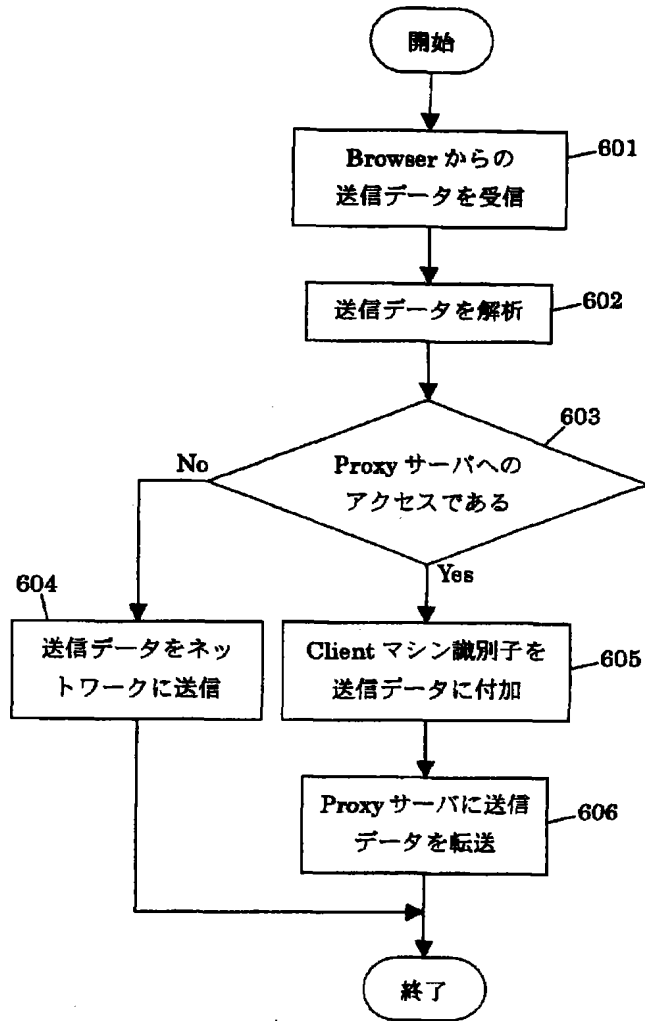


【図15】

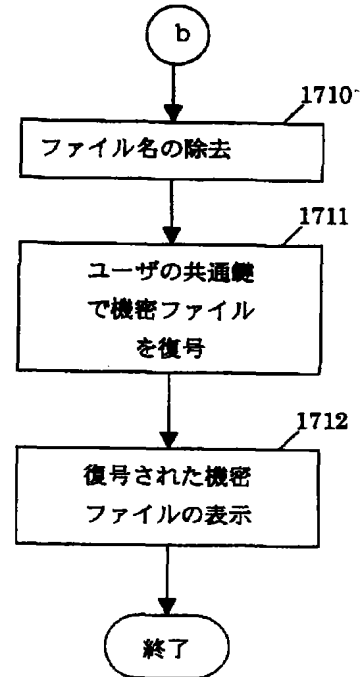


【図6】

通信ブックモジュールにおいて、データ送信時における処理のフローチャート

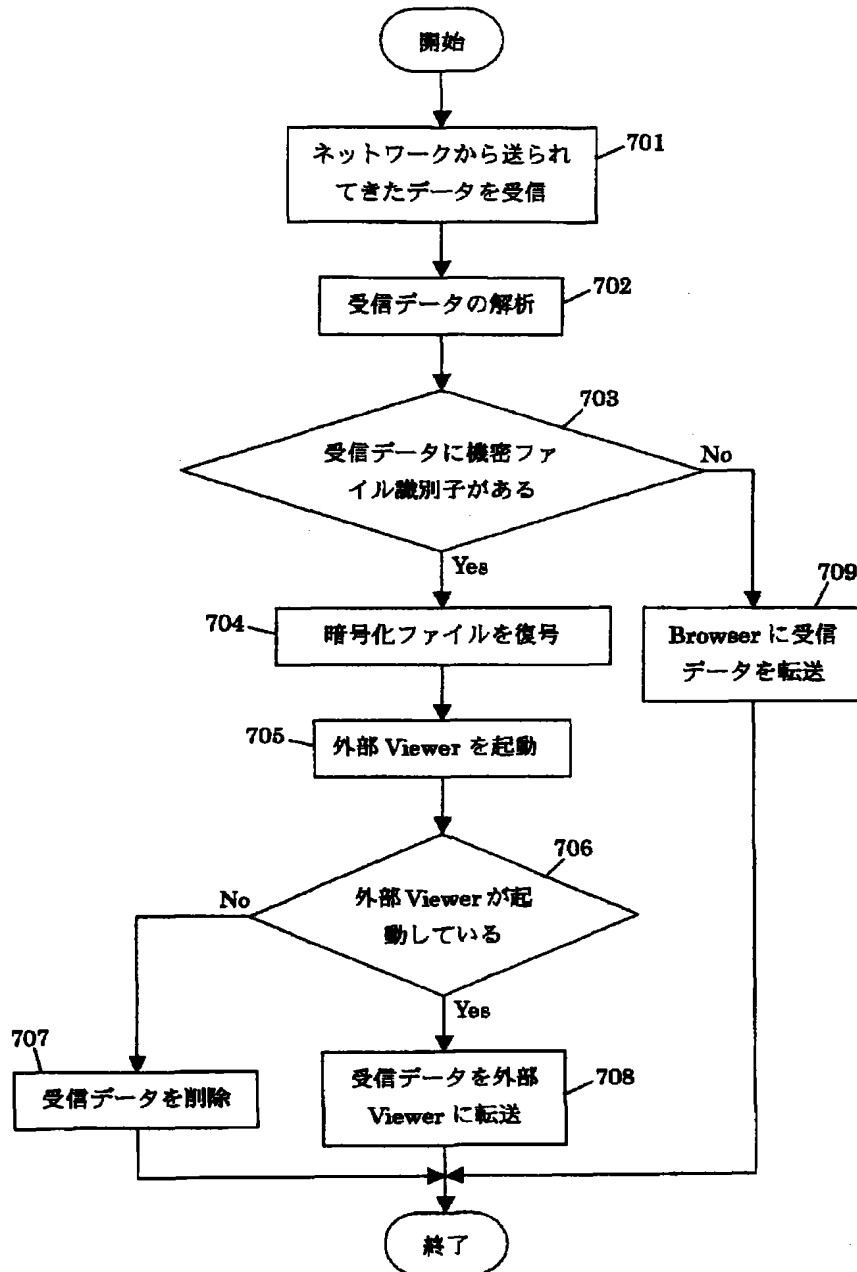


【図18】



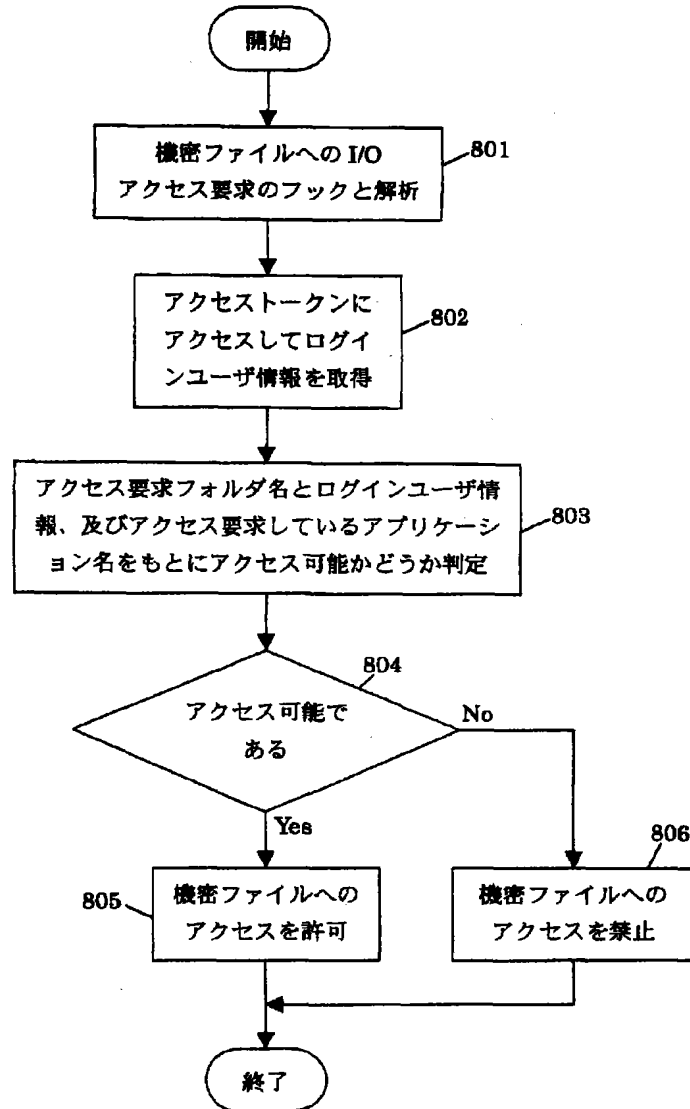
【図7】

通信フックモジュールにおいて、データ受信時における処理のフローチャート



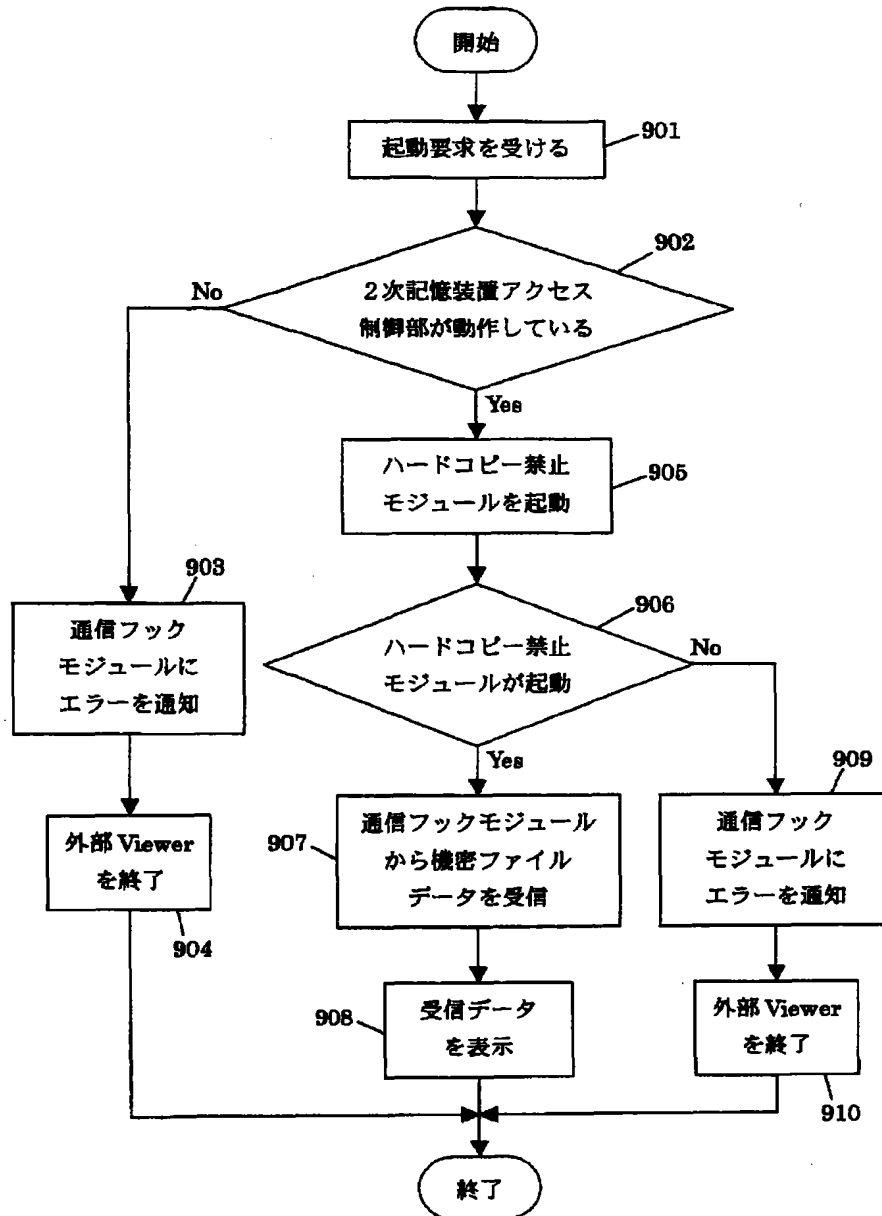
【図8】

2次記憶装置アクセス制御部における機密ファイルアクセス時の処理のフローチャート

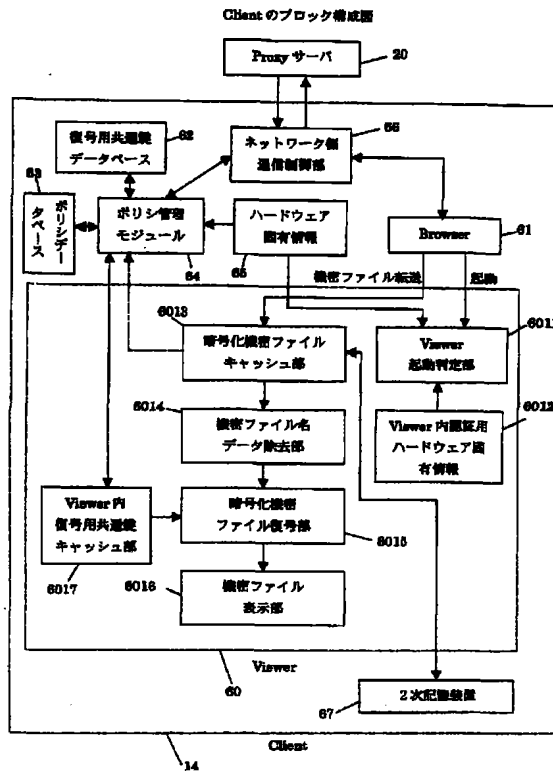


【図9】

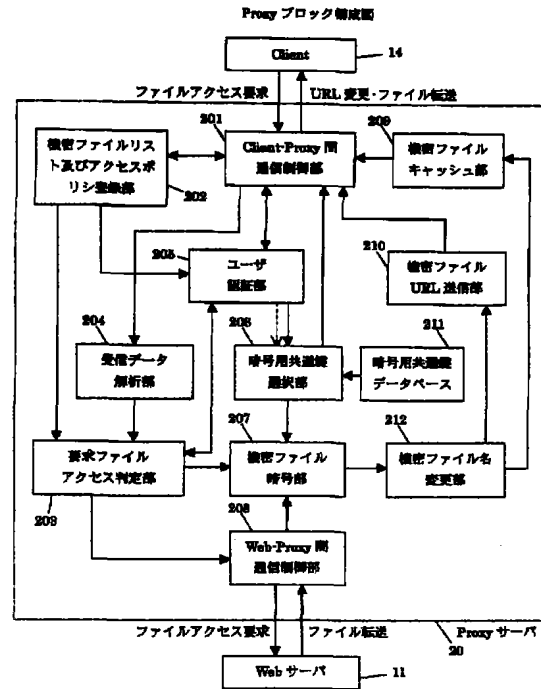
外部 Viewer における受信データ表示処理のフローチャート



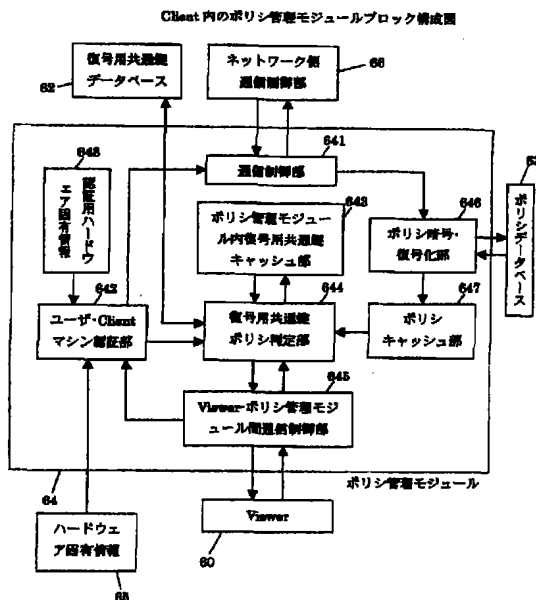
【図11】



【図12】

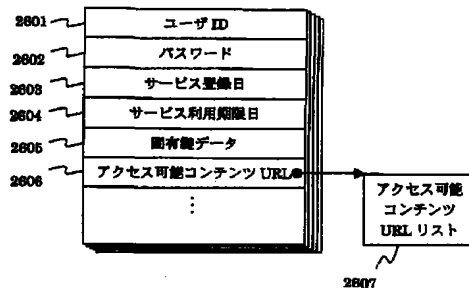


【図13】



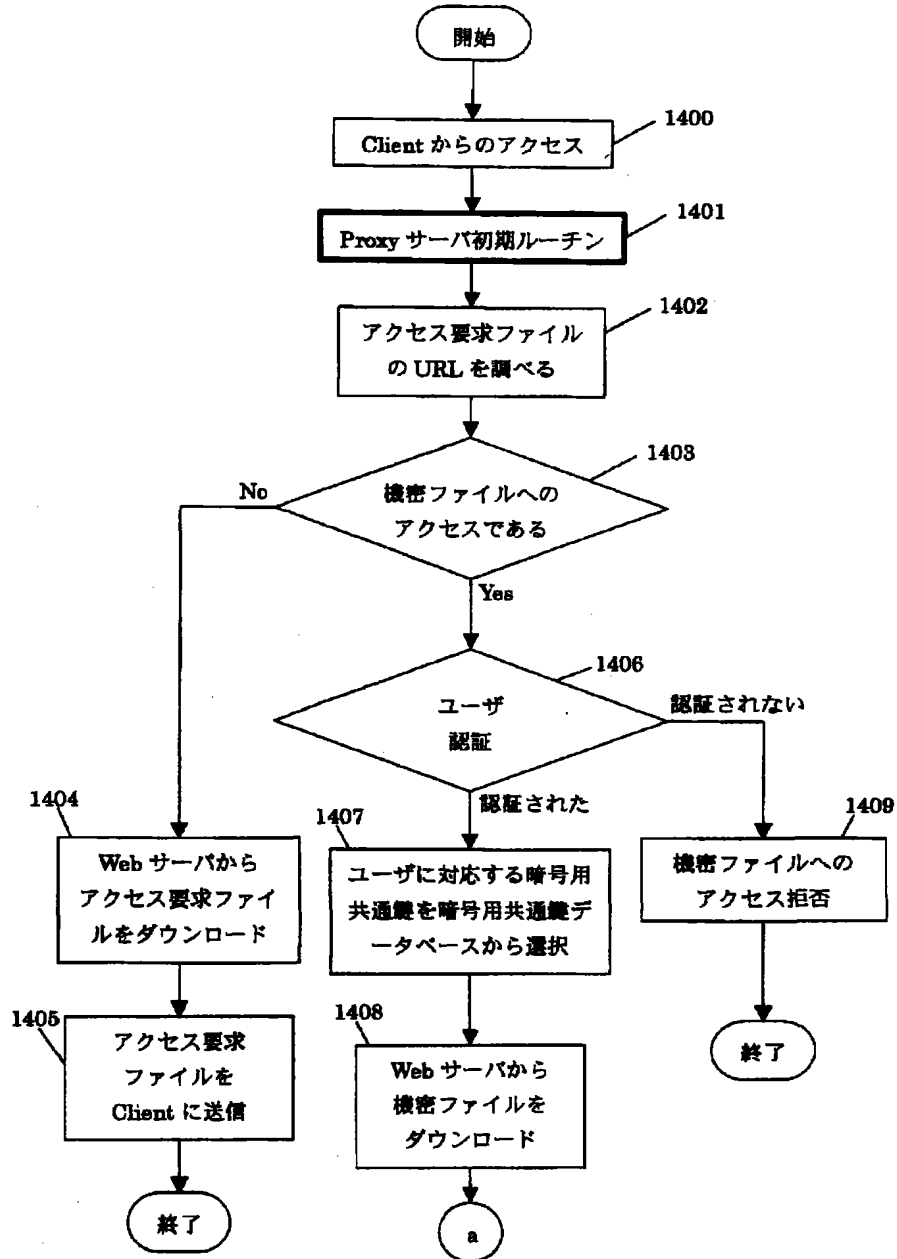
【図26】

ユーザ情報・固有IDに記録された  
アクセス可能な利用者のユーザ情報の概要構成図



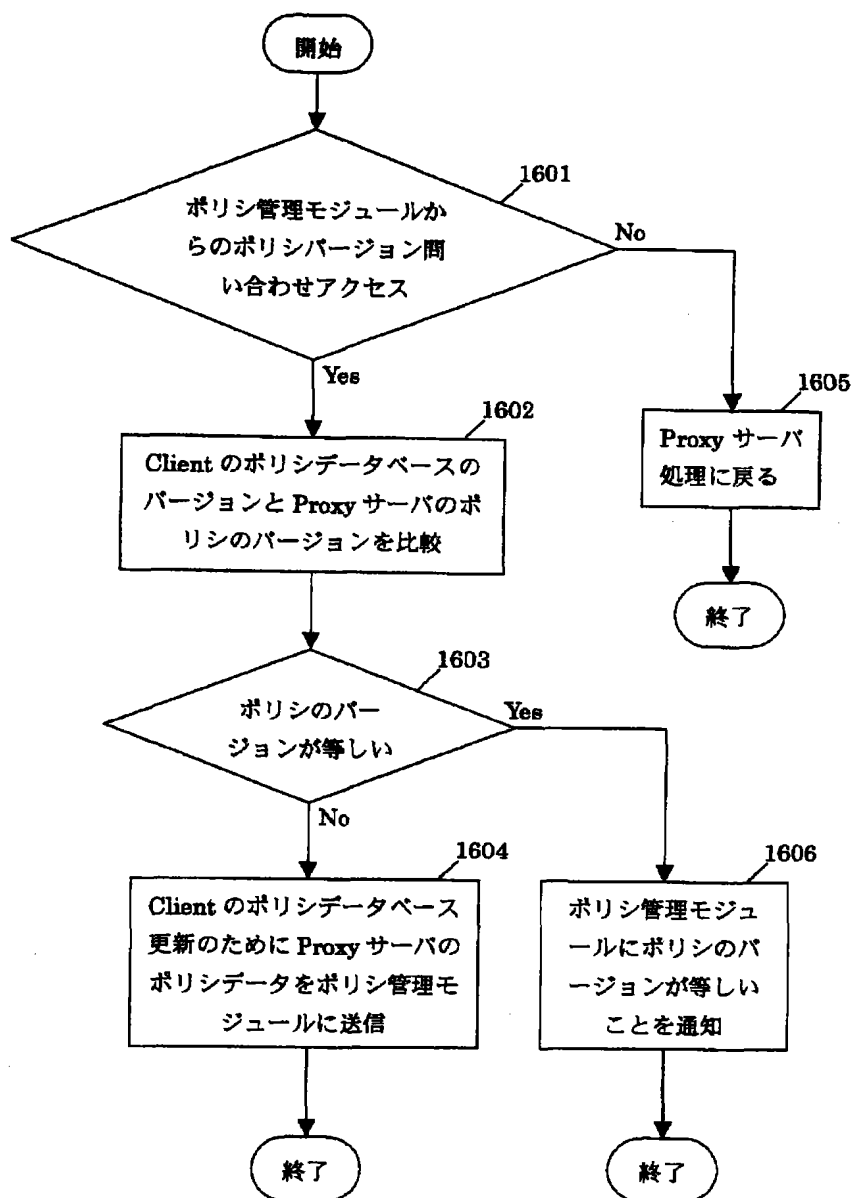
【図14】

Proxy サーバにおける処理のフローチャート



【図16】

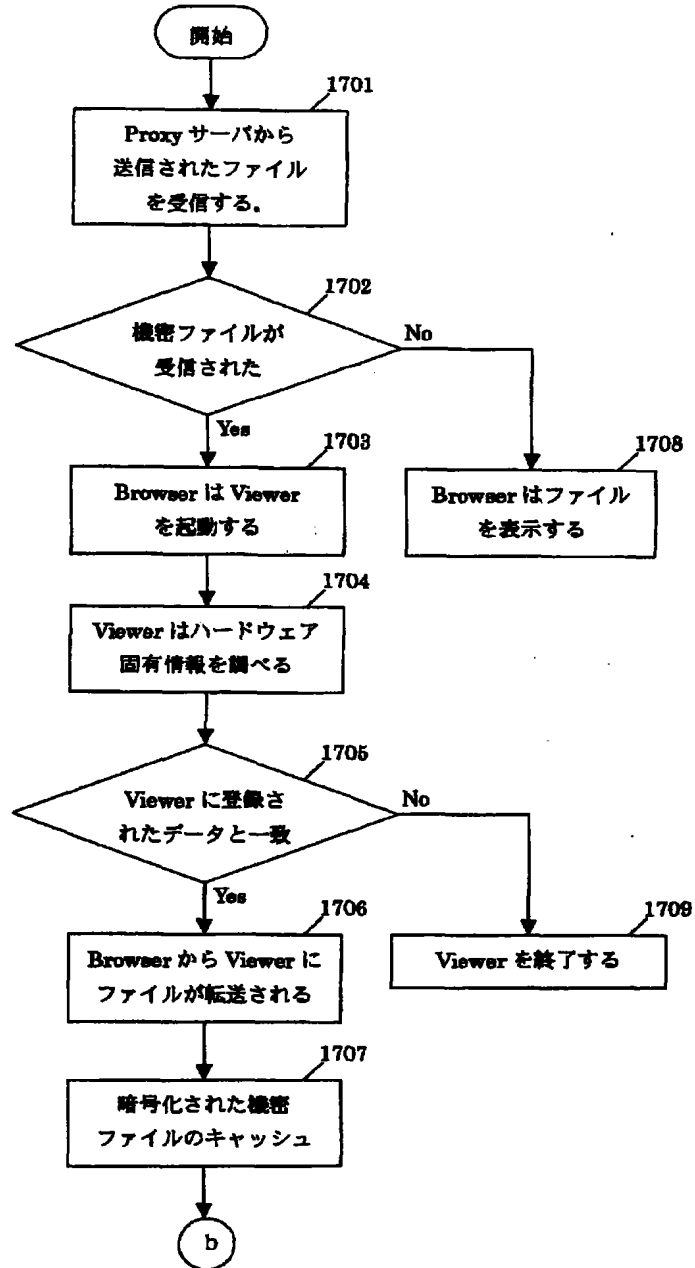
## Proxy サーバ初期ルーチンフローチャート





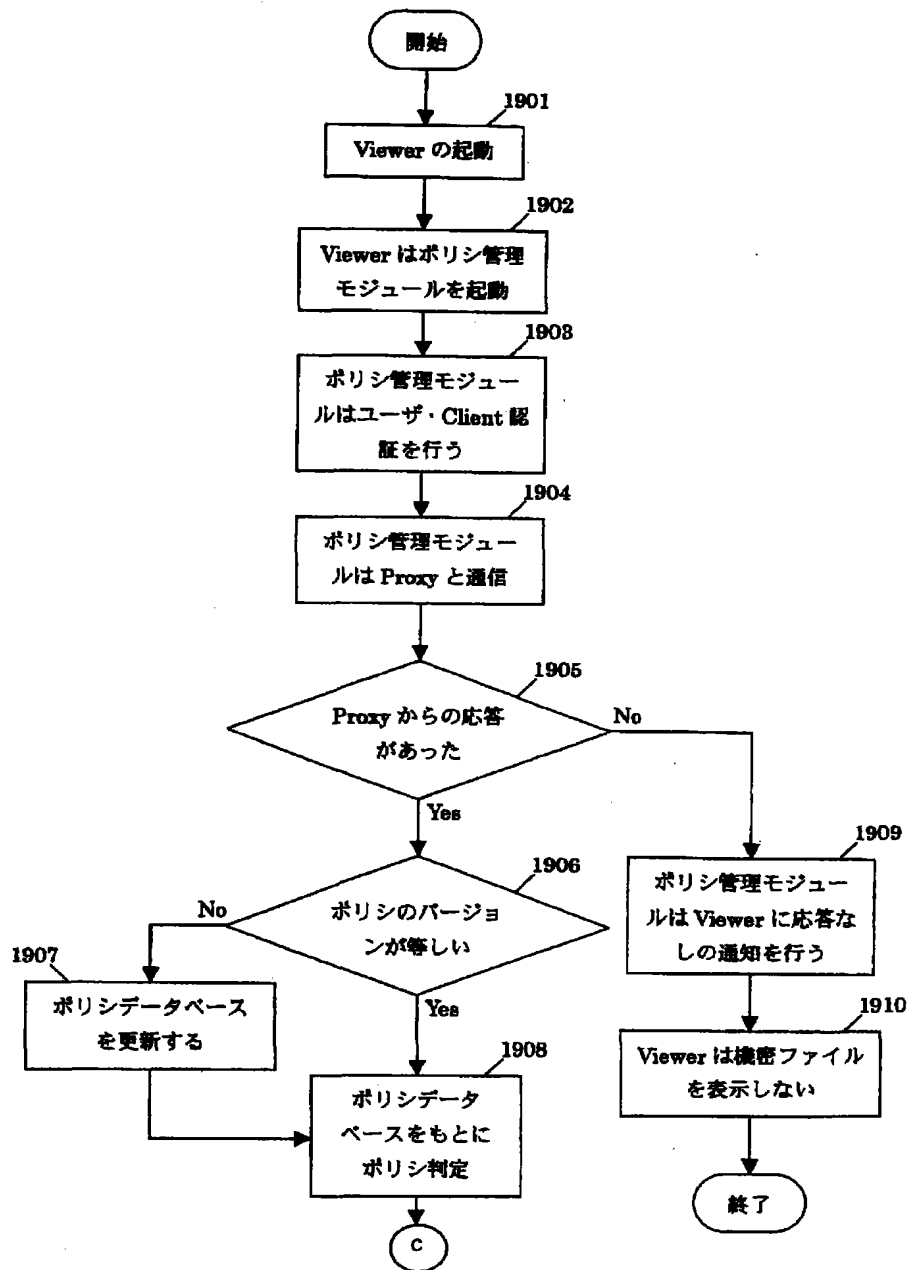
【図17】

Webサーバ上のファイル参照時のClientにおける処理のフローチャート

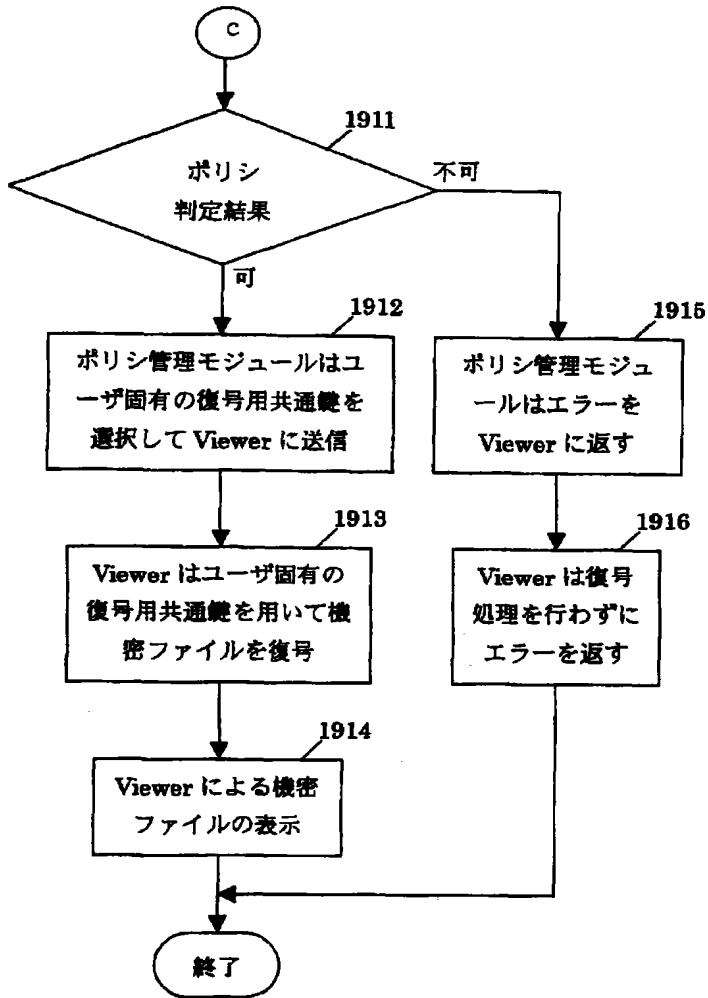


【図19】

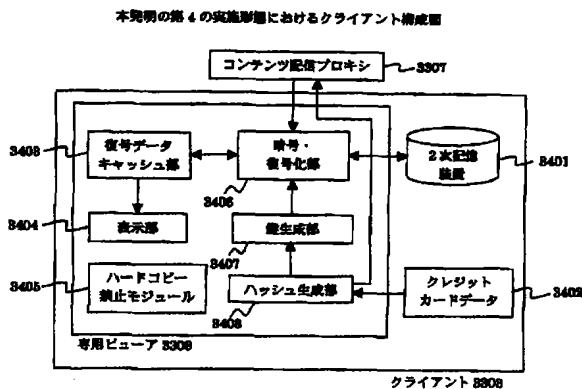
2次記憶装置に保存された機密ファイル参照時の Client における処理



【図20】



【図34】



【図31】

専用ビューアを使用してデジタルコンテンツ配信サービスに登録する際のインターフェイスの移り変わりを表した図

Screenshot of the registration page (Figure 31). The page is titled 'デジタルコンテンツ配信登録ページ' (Digital Content Distribution Registration Page). It contains a form with the following fields: '氏名' (Name), '性別' (Gender), '住所' (Address), 'メールアドレス' (Email address), 'クレジットカード番号' (Credit card number), '登録するユーザID・パスワード' (User ID and Password to be registered), 'ユーザID' (User ID), 'パスワード' (Password), and '入力確認' (Input confirmation). Below the form, there are checkboxes for 'コンテンツ項目 (利用したいコンテンツをチェック)' (Content items (check the content you want to use)): '本パールの人々' (People of this pearl), 'ヒマラヤの山々' (Mountains of the Himalayas), 'アンデス山脈' (Andes mountain range), '古代中国の道' (Ancient China's road), and '...' (Others). The page has 'OK' and '戻る' (Back) buttons.

Screenshot of the input confirmation page (Figure 31). The page is titled '入力情報の確認' (Input information confirmation). It displays the entered information: '氏名: 山崎 伸' (Name: Yamazaki Nobu), '性別: 男' (Gender: Male), '住所: 東京都中央区日本橋 XXX 町 8-10' (Address: 8-10, Nipponbashi, Chuoh-ku, Tokyo), 'メールアドレス: yamazaki@xxx.com' (Email address: yamazaki@xxx.com), 'カード番号: 1234 - 5678 - 1234 - 5678' (Card number: 1234 - 5678 - 1234 - 5678), 'ユーザ ID: yamazaki' (User ID: yamazaki), and 'パスワード: 非表示' (Password: Hidden). It also shows the selected content items: '選択コンテンツ: ヒマラヤの山々, アンデス山脈' (Selected content: Himalayas, Andes mountain range). The page has '戻る' (Back), '確定' (Confirm), and '中止' (Cancel) buttons.

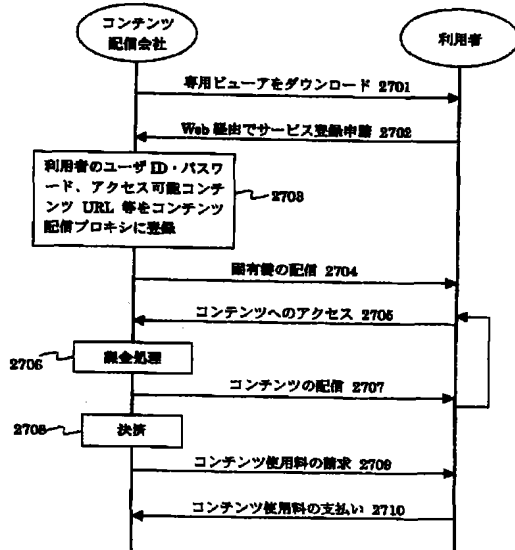
【図32】

Screenshot of the download progress page (Figure 32). The page is titled '登録完了ページ' (Registration completion page). It displays a progress bar and the text '登録完了ページ' (Registration completion page). The page has a 'キャンセル' (Cancel) button.

Screenshot of the completion page (Figure 32). The page is titled '登録完了ページ' (Registration completion page). It displays the text '登録完了しました。あなたのユーザ ID は以下のとおりです。' (Registration is complete. Your user ID is as follows.) and 'ユーザ ID: yamazaki' (User ID: yamazaki). It also displays the text '登録されたパスワードはメールで送信しました。パスワードを忘れた場合はヘルプデスクまでメールでおたずねください。' (The registered password has been sent by email. If you forget the password, please email the help desk.) The page has a '戻る' (Back) button.

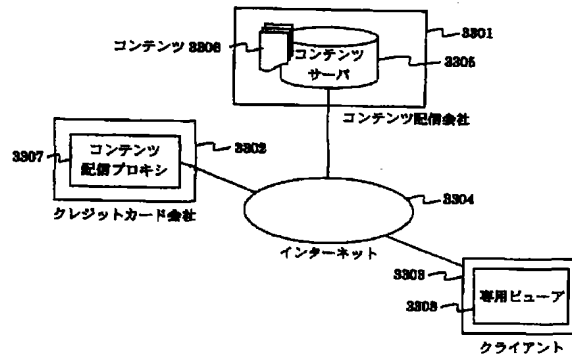
【図27】

コンテンツ配信サービスにおける全体の流れを時系列で示した図



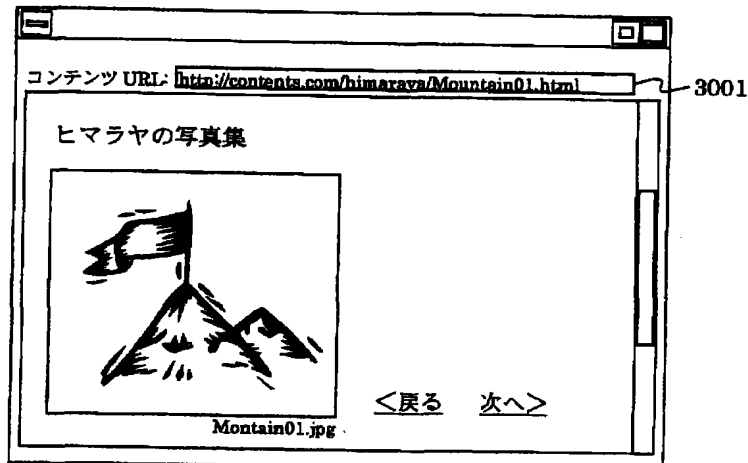
【図33】

本発明におけるデジタルコンテンツ配信システムの第4の実施形態を示した全体構成図



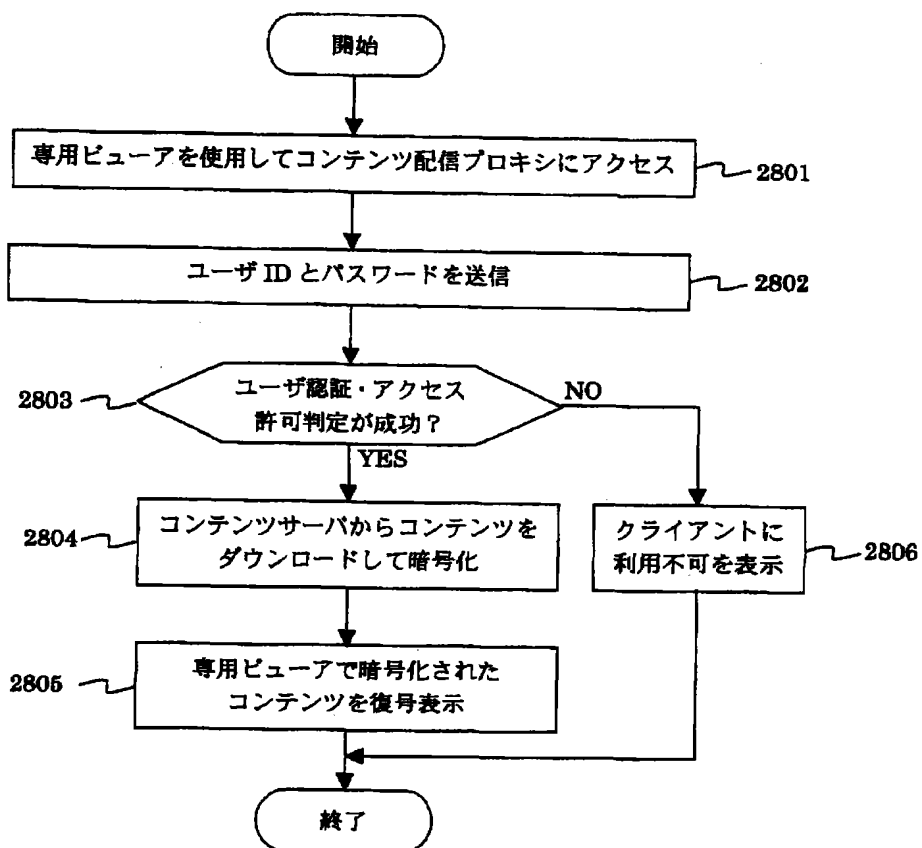
【図30】

専用ビューアインターフェイス図



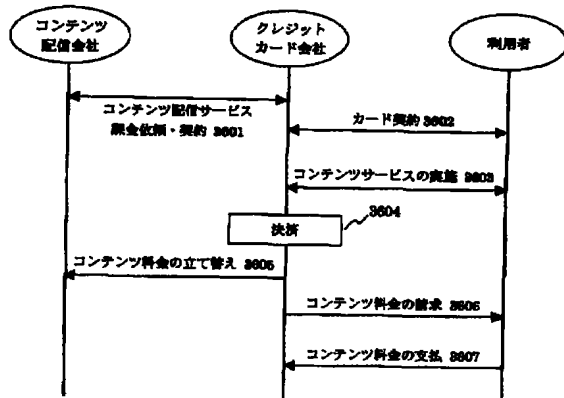
【図28】

コンテンツをダウンロードして専用ビューアで閲覧する際のフローチャート



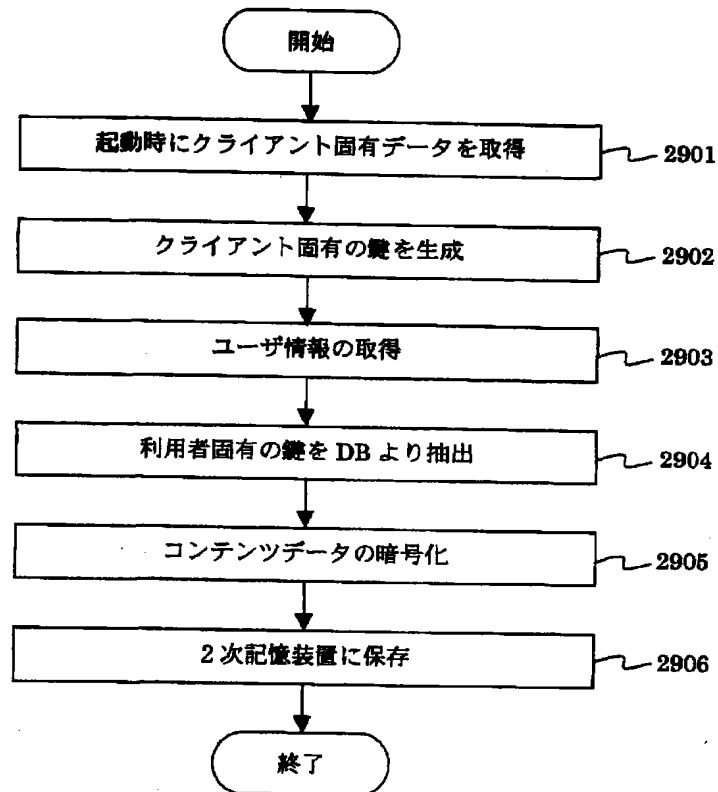
【図36】

コンテンツ配信サービス全体の流れを時系列で示した図

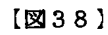


【図29】

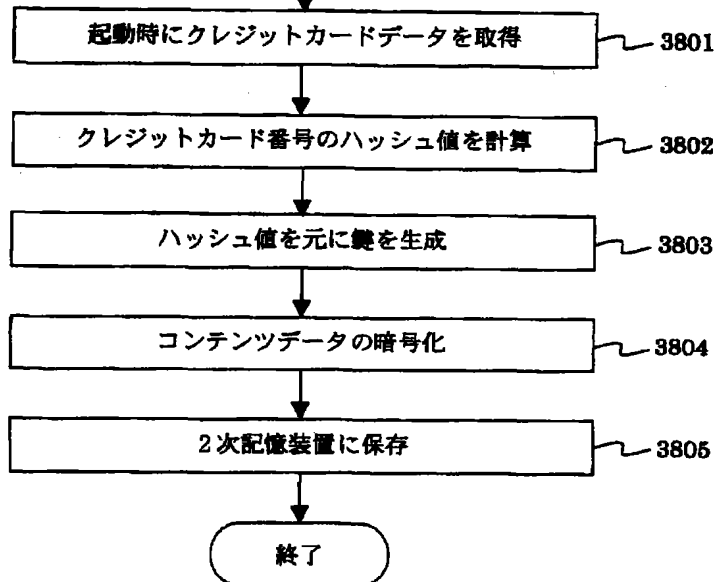
クライアントにコンテンツデータを保存する際の  
専用ビューアが行う処理のフローチャート



本発明の第 4 の実施形態におけるコンテンツ配信プロキシ構成図

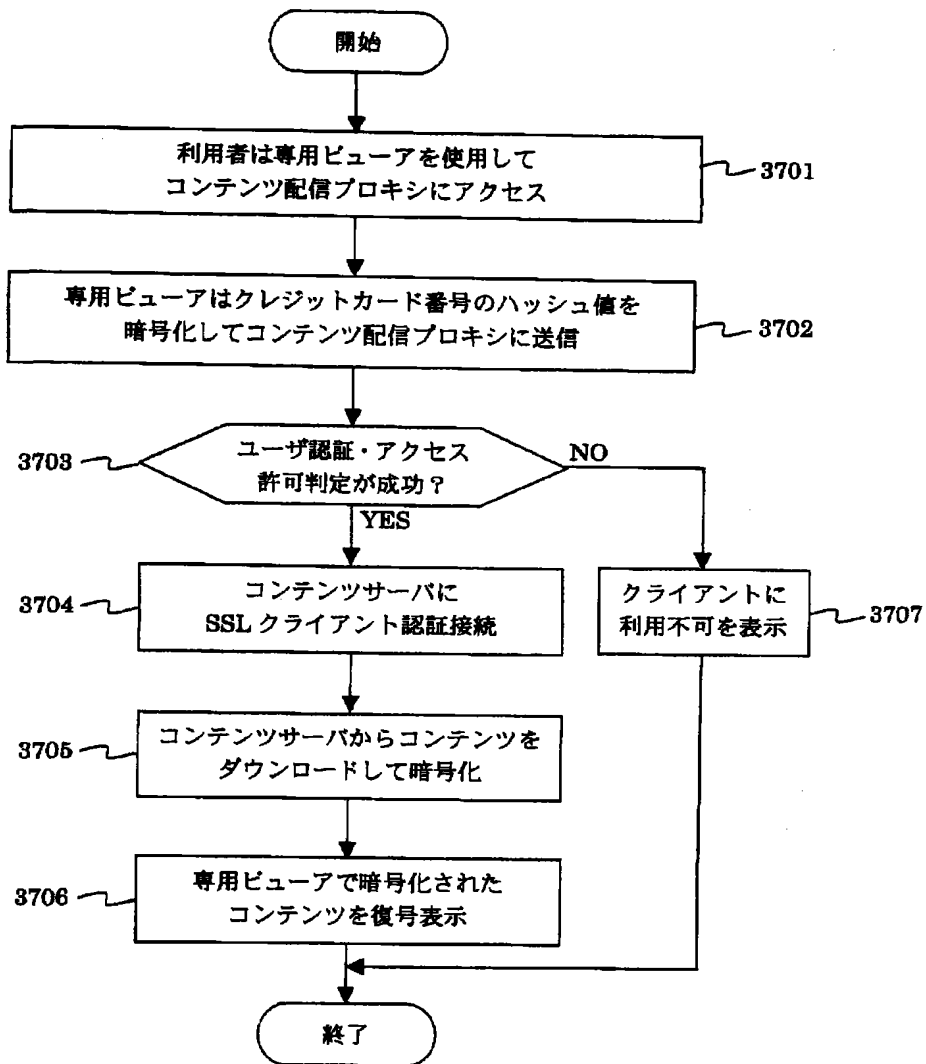


開始



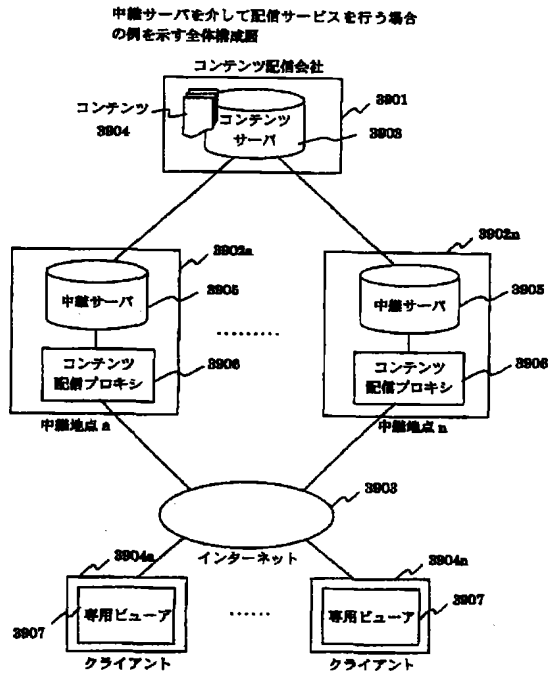
【図37】

コンテンツをダウンロードして専用ビューアで閲覧  
する際のシステム全体のフローチャート





【図39】



【図40】

